STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1953 - 013

Voordracht in de serie Actualiteiten

Dr. W. Peremans

26 september 1953

Some applications of lattice theory in algebra

1953

Voordracht door Dr W.Peremans in de serie Actualiteiten
op 26 September 1953.

Some applications of lattice theory in algebra.

We begin this conference with some well-known facts of lattice theory.

A *partially ordered set* P is a set with a relation $a \leq b$, satisfying the following three postulates:

(1) $a \leq a$.

(2) $a \leq b$ and $b \leq c$ imply $a \leq c$.

(3) $a \leq b$ and $b \leq a$ imply $a = b$.

In general for two elements a and b neither $a \leq b$, nor $b \leq a$ needs to hold. In this case we call a and b *incomparable*. If in a partially ordered set P for every pair a,b of elements either $a \leq b$ or $b \leq a$ holds, P is called a *simply ordered set* or a *chain*.

If, given two elements a and b of a partially ordered set P, there exists an element c satisfying $c \leq a$, $c \leq b$, and $x \leq a$, $x \leq b$ imply $x \leq c$, then c is called the *greatest lower bound* (g.l.b.) or the *meet* of a and b, and written $a \cap b$. Obviously two elements have at most one g.l.b. Similarly one defines the *least upper bound* (l.u.b.) or the *join* $a \cup b$ of a and b. So we have

(4) $a \cap b \leq a$.

(5) $a \cap b \leq b$.

(6) $x \leq a$ and $x \leq b$ imply $x \leq a \cap b$.

(7) $a \leq a \cup b$.

(8) $b \leq a \cup b$

(9) $a \leq x$ and $b \leq x$ imply $a \cup b \leq x$.

A partially ordered set satisfying the condition, that for every pair a,b of elements $a \cap b$ and $a \cup b$ exist, is called a *lattice*.

The following relations are valid for meet and join:

(10) $a \cap a = a$.

(11) $a \cap b = b \cap a$.

(12) $(a \cap b) \cap c = a \cap (b \cap c)$.

(13) $a \cup a = a$.

(14) $a \cup b = b \cup a$.

(15) $(a \cup b) \cup c = a \cup (b \cup c)$.

(16) $a \cup (a \cap b) = a$.

(17) $a \cap (a \cup b) = a$.

(18) $a \cup b = a$ implies $a \cap b = b$.

(19) $a \cap b = a$ implies $a \cup b = b$.

A lattice may also be defined as a set with two binary operations $\cap$ and $\cup$, satisfying the postulates (11), (12), (14), (15), (16) and (17). If $a \leq b$ is defined by $a \cap b = a$, the relation $\leq$ is a partial ordering, for which the given operations $\cap$ and $\cup$ are the meet and the join. Instead of (11), (12), (14), (15), (16) and (17), one can also take (10), (11), (12), (13), (14), (15), (18) and (19) as postulates.

A subset Q of a partially ordered set P is also a partially ordered set with respect to the same order relation. If P is a lattice with meet $\cap$ and join $\cup$, Q needs not to be a lattice. Q may even be a lattice with meet $\wedge$ and join $\vee$ different from the meet and join of P. Obviously in this case if $a \in Q$ and $b \in Q$, then $a \wedge b \leq a \cap b$ and $a \vee b \geq a \cup b$. We call Q a <u>sublattice</u> of P only if the meet- and join-operations in Q are the same as in P.

Example. Let V be a set and Φ a family of subsets of V. If $A \in \Phi$ and $B \in \Phi$, then $A \leq B$ is defined by $A \subseteq B$ (set-inclusion). With respect to this relation Φ is a partially ordered set. If Φ is the family of <u>all</u> subsets of V, Φ is a lattice, in which $A \cup B$ is the union and $A \cap B$ is the intersection of the sets A and B. If we take for V a group and for Φ the family of the subgroups of V, Φ also is a lattice, in which $A \cap B$ is the intersection of A and B, but $A \cup B$ is the subgroup generated by A and B, which in general is a set, which contains the set-union of A and B as a proper subset.

If V is a subset of a partially ordered set P and c is an element of P, such that $c \leq x$ for all $x \in V$, and $y \leq x$ for all $x \in V$ implies $y \leq c$, c is called the greatest lower bound inf V of V. Similarly the least upper bound sup V of V is defined. If one takes for V a set consisting of one or two elements, one gets the ordinary meet and join.

If P is a partially ordered set such that inf V and sup V exist for every non-void subset V of P, P is called a <u>complete lattice</u>

An element a of a partially ordered set P is called the <u>greatest</u> element of P, if $x \leq a$ for all $x \in P$. An element a of a partially ordered set P is called a <u>maximal</u> element of P if $a \lneq x$ holds for no $x \in P$. Similarly <u>least</u> and <u>minimal</u> elements are defined. If P contains a greatest element a, a is the only maximal element. In a chain the concepts of greatest and maximal element coincide. A complete lattice P has a greatest element (viz. sup P) and a least element (viz. inf P). Usually the greatest element (if it exists) of a partially ordered set is denoted by I and the least element (if it exists) by O.

<u>Theorem 1</u>. A partially ordered set with a greatest element I, and such that inf V exists for all non-void subsets of P is a complete lattice.

<u>Proof</u>: It is sufficient to prove the existence of sup V for an arbitrary non-void subset V of P. Take the set W, consisting of those elements $y \in P$, for which $x \leq y$ holds for all $x \in V$. Then W is non-void,

because $I \in W$. So $c = \inf W$ exists. If $x \in V$, $x \leq y$ holds for all $y \in W$, so $x \leq c$. Furthermore, if for $y \in P$ one has $x \leq y$ for all $x \in V$, then $y \in W$, so $c \leq y$. This proves $c = \sup V$.

A family Φ of subsets of a set V is said to satisfy the <u>intersection-property</u>, if for every non-void subfamily Ψ of Φ we have $\bigcap_{W \in \Psi} W \in \Phi$, $\bigcap$ being the sign for set-intersection.

From theorem 1 it follows that a family Φ of subsets of a set V, which satisfies the intersection-property and for which $V \in \Phi$ holds, is a complete lattice with respect to set-inclusion, for which $\inf \Psi = \bigcap_{W \in \Psi} W$ for every $\Psi \subseteq \Phi$.

From this we infer that the subgroups of a group, the normal subgroups of a group, the ideals of a ring, the left ideals of a ring, the right ideals of a ring, the subfields of a field, the closed subspaces of a topological space form complete lattices.

In the following we restrict ourselves to families of sets satisfying these properties.

A family Φ of subsets of a set V is said to satisfy the <u>union-property</u>, if for every non-void subfamily Ψ of Φ which is a chain, we have $\bigcup_{W \in \Psi} W \in \Phi$, $\bigcup$ being the sign for set-union.

The above-mentioned algebraic examples all satisfy the union-property. The closed subspaces of a topological space, however, in general do not satisfy this property.

In lattice theory properties of lattices are investigated; in particular lattices which satisfy additional requirements, such as modular lattices, distributive lattices, complemented lattices and so on. The results of this theory may then be applied in those branches of algebra, where these additional requirements hold. So e.g. the ideals of a ring forming a modular lattice the theory of modular lattices may be applied to the ideal lattice of a ring.

In a recent publication (Trans. Amer. Math. Soc. <u>75</u> (1953), 136-153) R.L.Blair applied lattice theory to the theory of rings in a somewhat different way. He investigated the consequences of imposing requirements on the ideal lattice of a ring which in general are not satisfied by this lattice, in this way restricting the class of rings under consideration. In doing this ring-theoretical properties may be found with the use of lattice theory and ring theory both. With this method he treats complementedness and distributivity. In the following we shall discuss some of his results on complementedness and make some remarks on pseudo-complementedness.

A lattice is called a <u>modular lattice</u> if

(20) $a \leq b$ implies $(a \cup c) \cap b \leq a \cup (c \cap b)$.

In every lattice $a \cup (c \cap b) \leq (a \cup c) \cap b$ holds, so in a modular lattice

(21) $a \leq b$ implies $(a \cup c) \cap b = a \cup (c \cap b)$.

The lattice of the subgroups of an abelian group is easily seen to be modular. The lattice of the ideals of a ring is a sublattice of the lattice of the subgroups of the additive group of the ring (the sum of two ideals being an ideal) and so, the sublattice of a modular lattice being modular, is a modular lattice.

A lattice L with a greatest element I and a least element O is called <u>complemented</u> if for every $a \in L$, there exists an $a' \in L$, such that $a \cap a' = O$, $a \cup a = I$. We call a' the complement of a. A lattice L is called relatively complemented if for every $a \in L$, $b \in L$, $x \in L$ with $a \leq x \leq b$ there exists an $y \in L$, such that $x \cap y = a$, $x \cup y = b$. We call y the complement of x relative to a and b.

A complemented modular lattice is relatively complemented. The complement of x relative to a and b is $(a \cup x') \cap b$, which is the same element as $a \cup (x' \cap b)$.

An element a of a lattice is called <u>meet-irreducible</u> if $a = b \cap c$ implies $a = b$ or $a = c$.

An element a of a lattice is called a <u>point</u> if $a \neq O$ and $x \leq a$ implies $x = O$ or $x = a$.

Blair proves the following theorem:

<u>Theorem 2</u>. If L is a complete complemented modular lattice with at least two elements, and if each element of L is the g.l.b of a set of meet-irreducible elements, then the greatest element I of L is a join of points.

Now we shall prove the well-known fact that the ideal lattice of a ring has the property that each element is the g.l.b. of a set of meet irreducible elements. For the proof of this theorem we make use of a theorem of Zorn, which is equivalent with the axiom of choice of set theory.

<u>Theorem 3</u>. (Zorn). If a non-void partially ordered set P has the property that for every non-void subset V of P, which is a chain, an element c exists with $x \leq c$ for all $x \in V$, then P contains a maximal element.

<u>Theorem 4</u>. If a family Φ of subsets of a set V satisfies the intersection-property and the union-property and if $V \in \Phi$, then every element of Φ is the g.l.b. of meet-irreducible elements of Φ.

<u>Proof</u>: Let $A \in \Phi$. Take the subfamily Ψ of Φ, consisting of those meet-irreducible elements W of Φ, for which $A \subseteq W$ holds. The family Ψ is non-void, because $V \in \Phi$. For the intersection $X = \bigcap_{W \in \Psi} W$ we have $A \subseteq X$. Take an element $c \in V$, $c \notin A$ and the subfamily Ω of Φ, consisting of those elements U of Φ, for which $A \subseteq U$ and $c \notin U$.

The family Ω is non-void, because $A \in \Omega$. Furthermore Ω satisfies the condition of Zorn's theorem, because the set-union L of a subchain of Ω is an element of Φ, for which $A \subseteq L$ and $c \notin L$ holds, so $L \in \Omega$. By Zorn's theorem Ω has a maximal element Y. Suppose $Y = R \cap S$, $R \in \Phi$, $S \in \Phi$. Then we have $A \subseteq R$, $A \subseteq S$. Moreover $c \notin R$ or $c \notin S$, for if $c \in R$ and $c \in S$ would hold both, $c \in Y$ would also hold, contrary to $Y \in \Omega$. So $R \in \Omega$ or $S \in \Omega$, so by the maximality of Y in Ω, $R = Y$ or $S = Y$. So Y is meet-irreducible in Φ and $A \subseteq Y$, so $Y \in \Psi$, so $X \subseteq Y$. As $c \notin Y$, we have $c \notin X$. This proves $X \subseteq A$; we had already found $A \subseteq X$, so $A = X$, which finishes the proof.

We have already seen that the ideal lattice of a ring satisfies the conditions of theorem 4, so in this lattice every element is the g.l.b. of meet-irreducible elements. If the ideal lattice is complemented, we may apply theorem 2. Now a point of the ideal lattice is called in ring-theoretical language a minimal ideal, so we find that if the ideal lattice is complemented, the ring is the sum of its minimal ideals. The converse of this theorem is a direct consequence of a well-known lattice-theoretical theorem.

Theorem 5. (Blair). A ring has a complemented ideal lattice if and only if it is the sum of its minimal ideals.

With a usual method of ring theory a sum of minimal ideals may be refined to a (discrete) direct sum.

It is perhaps of some interest to point out a terminological difficulty involved by the concept of direct sum. For the sake of simplicity we give the definition of direct sum for a finite number of summands.

A ring R is called the (inner) direct sum of its subrings $S_1, \ldots, S_n$, if there exists an isomorphism Λ between R and the ring R' consisting of the n-tuples $(s_1, \ldots, s_n)$ where $s_j \in S_j$, and where addition and multiplication is defined by $(s_1, \ldots, s_n) + (t_1, \ldots, t_n) = (s_1+t_1, \ldots, s_n+t_n)$ and $(s_1, \ldots, s_n)(t_1, \ldots, t_n) = (s_1t_1, \ldots, s_nt_n)$; furthermore Λ transforms an element $c \in S_j$ into $(0, \ldots, 0, c, 0, \ldots, 0)$ with c in the j^{th} place and zeros elsewhere. R' is called the outer direct product of $S_1, \ldots, S_n$. In a similar way the direct product of an infinite number of summands is defined. Direct summands of a ring are ideals in it.

The sum of a family Φ of ideals of a ring is the ideal generated by the ideals in Φ. It consists of those elements of the ring which may be written as a finite sum of elements of ideals belonging to Φ.

Now with these definitions of sum and of direct sum the direct sum of an infinite number of rings is in general not the sum of those rings, but contains the sum as a proper subset, viz. the subset of the elements with only a finite number of components $\neq 0$. This subset is usually called the discrete direct sum of the given summands. Perhaps it would be better to use in this case the term "direct sum" and to call the above-mentioned direct sum "direct union". With this terminology a direct sum would be a sum.

We remark that in a similar way the lattice of right ideals may be treated, which yields the following theorem:

Theorem 6. (Blair). A ring has a complemented right ideal lattice if and only if it is the sum of its minimal right ideals.

Obviously this theorem remains valid if right is replaced by left in it both times it occurs.

We are now going to replace the concept of complementedness by that of pseudo-complementedness.

In a lattice L with a least element 0 an element a^* is called the pseudo-complement of the element a if $a \cap a^* = 0$ and if $a \cap x = 0$ implies $x \leq a^*$.

In a lattice L an element a^*b is called the pseudo-complement of the element a relative to the element b if $a \cap (a^*b) \leq b$ and if $a \cap x \leq b$ implies $x \leq a^*b$.

If in a lattice with a least element 0 each element has a pseudo-complement, the lattice is called pseudo-complemented

If in a lattice each ordered pair of elements has a relative pseudo-complement, the lattice is called relatively pseudo-complemented.

Obviously $a^* = a^*0$. Furthermore a^* may be defined as the greatest element x for which $a \cap x = 0$ and similarly for a^*b.

In Birkhoff's "Lattice theory" some properties of pseudo-complements are deduced for relatively pseudo-complemented lattices. However, it is possible to deduce them for pseudo-complemented lattices as will be shown in the following. This is a real generalization, because a relatively pseudo-complemented lattice is distributive and it is easy to give examples of pseudo-complemented lattices which are not even modular.

We now suppose our lattice to be pseudo-complemented. Then we have:

(22) $a \cap x = 0$ and $a \cap y = 0$ imply $a \cap (x \cup y) = 0$.

Proof: $x \leq a^*$ and $y \leq a^*$, so $x \cup y \leq a^*$, so $a \cap (x \cup y) \leq a \cap a^* = 0$ so $a \cap (x \cup y) = 0$.

(23) $a \leq a^{**}$.

Proof: This follows from $a \cap a^* = 0$.

(24) $a \leq b$ implies $b^* \leq a^*$.

Proof: $a \cap b^* \leq b \cap b^* = 0$, so $a \cap b^* = 0$, so $b^* \leq a^*$.

Applying (24) twice we get:

(25) $a \leq b$ implies $a^{**} \leq b^{**}$.

(26) $a^{***} = a^*$.

Proof: From (23) and (24) it follows that $a^{***} \leq a^*$; substituting a^* for a in (23) we get $a^* \leq a^{***}$, so $a^{***} = a^*$.

(27) $(a \cup b)^* = a^* \cap b^*$.

Proof: $a \cap a^* \cap b^* = 0$ and $b \cap a^* \cap b^* = 0$, so, using (22), we get $(a \cup b) \cap a^* \cap b^* = 0$, so $a^* \cap b^* \leq (a \cup b)^*$. The converse inequality is trivial: $a \leq a \cup b$ gives $(a \cup b)^* \leq a^*$, $b \leq a \cup b$ gives $(a \cup b)^* \leq$ $\leq b^*$, so $(a \cup b)^* \leq a^* \cap b^*$. So we have $(a \cup b)^* = a^* \cap b^*$.

(28) $a^* \cup b^* \leq (a \cap b)^*$.

Proof: $a \cap b \leq a$ gives $a^* \leq (a \cap b)^*$, $a \cap b \leq b$ gives $b^* \leq (a \cap b)^*$, so $a^* \cup b^* \leq (a \cap b)^*$.

The converse inequality of (28) is not valid in general (intuitionistic propositional calculus!).

(29) $(a \cap b)^{**} = a^{**} \cap b^{**}$.

Proof: $a \cap b \cap (a \cap b)^* = 0$, so $b \cap (a \cap b)^* \leq a^*$, so $b \cap (a \cap b)^* \cap a^{**} \leq a^* \cap a^{**} = 0$, so $b \cap (a \cap b)^* \cap a^{**} = 0$, so $(a \cap b)^* \cap a^{**} \leq b^*$, so $(a \cap b)^* \cap a^{**} \cap b^{**} \leq b^* \cap b^{**} = 0$, so $(a \cap b)^* \cap$ $\cap a^{**} \cap b^{**} = 0$, so $a^{**} \cap b^{**} \leq (a \cap b)^{**}$. The converse inequality is trivial: $a \cap b \leq a$ gives $(a \cap b)^{**} \leq a^{**}$, $a \cap b \leq b$ gives $(a \cap b)^{**} \leq$ $\leq b^{**}$, so $(a \cap b)^{**} \leq a^{**} \cap b^{**}$. So we have $(a \cap b)^{**} = a^{**} \cap b^{**}$.

We define the operation $\vee$ by $a \vee b = (a \cup b)^{**}$. Then we have $a \leq a \cup b \leq (a \cup b)^{**}$, $b \leq a \cup b \leq (a \cup b)^{**}$; if $a \leq x$, $b \leq x$ and $x^{**} = x$, then $a \cup b \leq x$, so $(a \cup b)^{**} \leq x^{**} = x$. If we call an element a <u>closed</u> if $a = a^{**}$ (or equivalently if $a = b^*$ for some b), then in the partially ordered set of closed elements the operation $\vee$ is the join-operation. Furthermore (29) yields that if a and b are closed, $a \cap b$ is closed too. So we find that the closed elements form a lattice.

The following two properties are obvious:

(30) $0^* = I$.

(31) $I^* = 0$.

Applying (27) and (30) we get $a \vee a^* = (a \cup a^*)^{**} = (a^* \cap a^{**})^* =$ $= 0^* = I$, so we have:

(32) $a \vee a^* = I$.

By definition we have $a \cap a^* = 0$, so in the lattice of closed elements a^* is a complement of a.

(33) $(a \cap b)^* = a^* \vee b^*$.

Proof: $(a \cap b)^* = (a \cap b)^{***} = (a^{**} \cap b^{**})^* = (a^* \cup b^*)^{**} = a^* \vee b^*$.

(34) $(a \vee b)^* = a^* \cap b^*$.

Proof: $(a \vee b)^* = (a \cup b)^{***} = (a \cup b)^* = a^* \cap b^*$.

A complemented lattice in which the complements satisfy (33) and (34) is called an <u>orthocomplemented</u> lattice. So the lattice of closed elements is orthocomplemented. Furthermore in this lattice every element has only one complement. For suppose we have elements a and a' with $a'^{**} = a'$, $a \cap a' = 0$, $a \vee a' = I$, then $a \cap a' = 0$ implies $a' \leq a^*$, so $a^{**} \leq a'^*$ and $a \vee a' = I$ implies $0 = I^* = (a \vee a')^* = a^* \cap a'^*$, so

$a'^* \leq a^{**}$. So we have $a'^* = a^{**}$ and therefore $a' = a'^{**} = a^{***} = a^*$.

A lattice is called a <u>distributive</u> lattice if it satisfies

(35) $a \cap (b \cup c) \leq (a \cap b) \cup (a \cap c)$.

In every lattice $(a \cap b) \cup (a \cap c) \leq a \cap (b \cup c)$ holds, so a distributive lattice satisfies

(36) $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$.

A complemented distributive lattice is called a <u>Boolean algebra</u>.

It is a well-known theorem of lattice theory that an orthocomplemented lattice, in which every element has only one complement, is a Boolean algebra (Birkhoff, Lattice theory, p. 171).

So we may conclude:

<u>Theorem 7</u>. The closed elements of a pseudo-complemented lattice form a Boolean algebra.

In Birkhoff's "Lattice theory" this theorem is proved only for pseudo-complemented distributive lattices.

If the ideal lattice of a ring R is pseudo-complemented and A is an ideal of R, obviously the pseudo-complement A^* of A is the sum of all ideals disjoint from A. Conversely if in a ring R the sum of all ideals disjoint from an ideal A is also disjoint from A, the ideal lattice of R is pseudo-complemented. So we have:

<u>Theorem 8</u>. If the ideal lattice of a ring R is pseudo-complemented the sum of the ideals of a family Φ of ideals of R with the property that $A \in \Phi$, $B \in \Phi$ and $A \neq B$ imply $A \cap B = 0$ (the zero ideal), is a discrete direct sum.

The lattice of closed elements in a pseudo-complemented lattice may be trivial. If a lattice L with 0 and I is such that the partially ordered set of elements $\neq 0$ has a least element, then L is pseudo-complemented with $a^* = 0$ for $a \neq 0$, and $0^* = I$. The only closed elements are 0 and I. In the ideal lattice of a ring R this is the case if R contains a least ideal $\neq 0$, which e.g. occurs in primitive rings with minimal right ideals, the sum of all minimal right ideals being such an ideal (cf. Jacobson, Amer. J. Math. <u>67</u> (1945), p. 317).