ON THE LATTICE THEORY OF IDEALS†

BY GARRETT BIRKHOFF

1. *Outline.* The ideals of any ring define, relative to g.c.f. and l.c.m., a combinatorial system having properties which we shall presently define as characterizing *B-lattices.*

In this article we shall first develop some new properties of B-lattices as abstract systems; the main results of this part of the work find expression in Theorems 1–5. Then we shall apply this theory and some older results to the ideals of commutative rings R which possess a principal unit l and satisfy the Basis Theorem. In addition to developing the known theory of *einartig* ideals by combinatory methods, we give a necessary and sufficient condition that the *B-lattice* defined by the ideals of R should be isomorphic with a *ring* of point sets in the sense of Hausdorff.‡

2. *Notation*; *Lattice Algebras.* We shall in general use capital letters to denote systems, and small letters for elements. $a \in A$ will mean "a is an element of the system A"; $B \subset A$ will mean "$b \in B$ implies $b \in A$"; $B < A$ will mean $B \subset A$ but $B \neq A$.

By a *lattice algebra* will be meant any system L which satisfies the following postulates:

(L1). Any $a \in L$ and $b \in L$ determine a unique "*join*" $a \cap b \in L$ and a unique "*meet*" $(a, b) \in L$.
(L2). $a \cap b = b \cap a$ and $(a, b) = (b, a)$ for any $a \in L$ and $b \in L$.
(L3). $a \cap (b \cap c) = (a \cap b) \cap c$ and $(a, (b, c)) = ((a, b), c)$ for any $a \in L$, $b \in L$, and $c \in L$.
(L4). $a \cap (a, b) = a$ and $(a, a \cap b) = a$ for any $a \in L$ and $b \in L$.

From (L1)–(L4) follow $a \cap a = (a, a) = a$. Moreover $a \cap b = b$ is equivalent to $(a, b) = a$; in this case we write $a \subset b$ or $b \supset a$, and $a \subset b$ taken with $b \subset c$ implies $a \subset c$. Moreover, $a < b$ means $a \subset b$ but $a \neq b$, while "b covers a" means $a < b$, but that no $x \in L$ satisfies $a < x < b$.

The reader may find it helpful to regard lattices as distorted

---

† Presented to the Society, March 30, 1934.

‡ Hausdorff, *Mengenlehre*, 1927, p. 77.

Boolean algebras in which $a \cap b$ is substituted for $a+b$, and (a, b) for $a \cdot b$.

The following additional conditions are optional:

(L5). If $a \subset c$, then $a \cap (b, c) = (a \cap b, c)$.
(L6). $(a, b \cap c) = (a, b) \cap (a, c)$ for any $a \in L$, $b \in L$, and $c \in L$.

If a lattice satisfies (L5), it is called a B-lattice; if it satisfies (L6), it is called a C-lattice. Any C-lattice is a B-lattice, and also satisfies $a \cap (b, c) = (a \cap b, a \cap c)$.

3. *Subdirect Decomposition.* We shall consider in §§3–4 only lattices L which have a *"largest"* element j satisfying $a \cap j = j$ for every $a \in L$; such is always the case in applications.†

We shall say that $a \in L$ and $b \in L$ are *coprime* if and only if $a \cap b = j$. We shall say that two sublattices‡ $A \subset L$ and $B \subset L$ are *coprime* if and only if $a \in A$ and $b \in B$ imply $a \cap b = j$. We shall say that the sublattices of a finite or transfinite§ sequence of sublattices $A_1 \subset L, \cdots, A_n \subset L$ are *strongly coprime* if and only if every A_i is coprime with the sublattice generated by|| the other sublattices of the sequence.

Let $B_1, \cdots, B_n$ be any (finite or transfinite) sequence of lattices, whose largest elements are $j_1, \cdots, j_n$. By an *f-type* vector $[b_1, \cdots, b_n]$, $(b_i \in B_i)$, we mean one in which $b_i = j_i$ except for a *finite* set of subscripts i. By the *subdirect product* $B_1 \hat{x} \cdots \hat{x} B_n = B^*$ of the B_i is meant the lattice whose elements are the f-type vectors just defined, and such that by definition

$$[b_1, \cdots, b_n] \cap [b_1', \cdots, b_n'] = [b_1 \cap b_1', \cdots, b_n \cap b_n'],$$

$$([b_1, \cdots, b_n], [b_1', \cdots, b_n']) = [(b_1, b_1'), \cdots, (b_n, b_n')].$$

B^* is evidently a lattice with largest element $[j_1, \cdots, j_n]$. Further, if B_i^* denotes the sublattice of elements of the form $[j_1, \cdots, j_{i-1}, b_i, j_{i+1}, \cdots, j_n]$ of B^*, then B_i^* is isomorphic with B_i, the lattices $B_1^*, \cdots, B_n^*$ are strongly coprime, and any element of B^* can be expressed as the meet of a finite num-

† In fact, if the number of elements of L is finite, this follows from (L1)–(L3.)

‡ A sublattice A of L is any subsystem such that $a \in A$ and $a' \in A$ imply $a \cap a' \in A$ and $(a, a') \in A$.

§ That is, in which the subscripts run through transfinite ordinals.

|| By the "sublattice generated by" is meant the least sublattice containing.

ber of elements in the various B_i^*. Finally, if the B_i are B-lattices, then so† is B^*.

Conversely, let B be any B-lattice, and let $B_1, \cdots, B_n$ be any finite or transfinite sequence of strongly coprime sublattices of B such that any $b \in B$ can be expressed as the meet $(b_{i_1}, \cdots, b_{i_m})$ of a finite number of $b_{i_k} \in B_{i_k}$.

For any $b \in B$ and $b' \in B$ we can evidently so reorder the B_i that $b = (b_1, \cdots, b_m)$, $b' = (b_1', \cdots, b_m')$, and $b \cap b' = b'' = (b_1'', \cdots, b_m'')$, where $b_i \in B_i$, $b_i' \in B_i$, $b_i'' \in B_i$, and m is finite. But by (L2)–(L3), we have

$$(b, b') = ((b_1, \cdots, b_m), (b_1', \cdots, b_m')) = ((b_1, b_1'), \cdots, (b_m, b_m')).$$

Further if we set $a_i = (b_i, b_i', b_i'')$, then

$$a_i \cap b'' = a_i \cap b \cap a_i \cap b' = a_i \cap (b_1, \cdots, b_m) \cap a_i \cap (b_1', \cdots, b_m'),$$

whence by (L5), setting $c_i = (b_1, \cdots, b_{i-1}, b_{i+1}, \cdots, b_m)$, and c_i' and c_i'' equal to the corresponding dashed expressions, we have

$$(a_i \cap c_i'', b_i'') = (a_i \cap c_i, b_i) \cap (a_i \cap c_i', b_i'),$$

whence, by strong coprimeness, after reduction, $b_i'' = b_i \cap b_i'$.

That is, B is a homeomorphic image of the subdirect product $B^* = B_1 \hat{x} \cdots \hat{x} B_n$. But if $b_i = b_i'$, and b^* in B^* is the image of (b_i, b_i') of B_i, then $b^* \cap [b_1, \cdots, b_n] = b_i \neq b_i' = b^* \cap [b_1', \cdots, b_n']$, whence, by (L1), $[b_1, \cdots, b_n] \neq [b_1', \cdots, b_n']$, and the homeomorphism is an isomorphism. In summary, we have proved the following theorem.

THEOREM 1. *A given B-lattice B (with largest element) is isomorphic with the subdirect product* $B_1^* \cdots B_n^*$ *(*B_i^* *any B-lattice with largest element) if and only if B contains strongly coprime sublattices* $B_1, \cdots, B_n$ *respectively isomorphic with* $B_1^*, \cdots, B_n^*$ *such that any* $b \in B$ *can be expressed as a meet* $(b_{i_1}, \cdots, B_{i_m})$, *where m is finite and* $b_{i_k} \in B_{i_k}$.

Notice that if n is finite, then a subdirect product is a direct product; while if $n = 2$, then strong coprimeness is equivalent to coprimeness.

4. *Uniqueness Theory.* Let L be any lattice (with a largest element), and suppose that L is isomorphic with two subdirect products $A_1 \hat{x} \cdots \hat{x} A_m$ and $B_1 \hat{x} \cdots \hat{x} B_n$. We know by the sec-

† The identical relations (L2)–(L5) can be checked seriatim.

ond paragraph of § 3, how to identify the A_i (and B_i) with strongly coprime sublattices of L in such a way that any element of L can be represented as the meet of a finite number of elements of the various A_i (or B_i). The reader can easily check the statement that, since $(a_i, a_j)=b_k$, $(b_k \in B_k)$, if and only if $a_i \in B_k$ and $a_j \in B_k$, each B_i is the subdirect product of its intersections with the various A_i; this proves the following statement.

THEOREM 2. *If* $L=A_1 \hat{x} \cdots \hat{x} A_m = B_1 \hat{x} \cdots \hat{x} B_n$ *is any lattice,*† *then* $L=F_{1,1}\hat{x} \cdots \hat{x} F_{m,n}$, *where* $A_i = F_{i,1}\hat{x} \cdots \hat{x} F_{i,n}$ *and* $B_j = F_{1,j}\hat{x} \cdots \hat{x} F_{m,j}$.

COROLLARY 1. *A lattice has at most one expression as a subdirect product of factors not themselves subdirect products.*

COROLLARY 2. *A finite lattice has a unique expression as the direct product of lattices not themselves direct products of lattices with fewer elements. The factors of any expression of the lattice as a direct product are direct products of the factors of this special decomposition into prime factors.*

These corollaries are of extremely general application.‡ We now assume in addition that L satisfies the following postulate.

(ϕ) Any sequence $a_1, a_2, a_3, \cdots$ of elements of L, such that $a_k < a_{k+1}$ for every k, is finite.

Well-order the expressions $L=L_1{}^i \hat{x} \cdots \hat{x} L_n{}^i$ of L as a subdirect product, and apply Theorem 2 iteratedly. If we concentrate our attention on the corresponding well-ordered set of meets $(a_1{}^i, \cdots, a_{\alpha_i}{}^i)=a$ representing a fixed $a \in L$ (each $a_h{}^i$ lying in just one of the $L_k{}^j$ for each $j \leqq i$, by Theorem 2), we see that the expression $(a_1{}^i, \cdots, a_{\alpha_i}{}^i)$ undergoes§ in virtue of (ϕ) at most a finite number of transmutations. Hence we can proceed through limit-numbers, and, by transfinite induction, we have the following result.

---

† By definition of subdirect product, either $m=n=1$ and the theorem is trivial, or the A_i, B_j, and L have largest elements.

‡ See Theorem 3.1 of the author's paper *On the combination of subalgebras*, Proceedings of the Cambridge Philosophical Society, vol. 29 (1933), pp. 441–464. This article will be cited in future references as "Subalgebras."

§ Each transmutation replaces an $a_h{}^i$ by the meet of $a_{h'}{}^{i+1} > a_h{}^i$ and $a_{h''}{}^{i+1} > a_h{}^i$.

THEOREM 3. *A lattice satisfying* (ϕ) *has one and only one expression as a subdirect product of factors not themselves subdirect products.*

Theorem 3 can evidently be applied to the ideals in rings which satisfy the ideal-chain theorem.

5. *Standard Exceptions to* (L6). Let B be any B-lattice, suppose g_1, g_2, and g_3 to be any three elements of B, and refer to Tables I–III of "Subalgebras"—only replacing A_i, B_i, M_i, N_i, C_i, F_i, and H_i by a_i, b_i, m_i, n_i, c_i, f_i, and h_i.

Suppose $c_i = c_j$ for some $i \neq j$. Then $a = (c_i, c_j) = c_i \cap c_j = b$, whence $(g_1, h_1) = (g_1, h_1, h_2, h_3) = (g_1, f_1 \cap f_2 \cap f_3) = (f_2 \cap f_3) \cap (g_1, f_1)$ [by (L5)] $= f_2 \cap f_3 \cap f = f_2 \cap f_3$, which is to say, $(g_1, g_2, \cap g_3) = (g_1, g_2) \cap (g_1, g_3)$. If therefore (L6) is violated at all, we must have some instance where the c_k are all distinct, yet $(c_i, c_j) = a$ and $c_i \cap c_j = b$ for $i \neq j$, whence $(c_1, c_2 \cap c_3) \neq (c_1, c_2) \cap (c_1, c_3)$. This proves the following fact.

THEOREM 4. *If a B-lattice is not a C-lattice, it contains a sublattice of order five and fixed structure not a C-lattice.*

Combining Theorem 4 with the result, due to Dedekind,† that any lattice not a B-lattice contains a sublattice of order five and fixed structure not a B-lattice, we get the following result.

COROLLARY. *If a lattice is not a C-lattice, it contains a sublattice of order five which is not a C-lattice.*

6. *Specialization by Induction.* Suppose B of §5 satisfies condition (ϕ) of §4, and consider the exception referred to in Theorem 4. We can by (ϕ) choose $c_1^* \supset c_1$ *covered* by b (see §2). Theorems 8.1 and 9.1 of "*Subalgebras*" show us successively that c_3 covers (c_1^*, c_3), $b = c_2 \cap c_3$ covers $c_2^* = c_2 \cap (c_1^*, c_3)$, hence c_1^* and c_2^* both cover $a^* = (c_1^*, c_2^*)$. Similarly $b = c_3 \cap c_2^*$ covers $c_3^* = c_3 \cap (c_1^*, c_2^*)$, and, since $c_3^* \supset a^*$, $(c_1^*, c_3^*) = (c_2^*, c_3^*) = a^*$. This proves the following theorem.

THEOREM 5. *If B is any B-lattice satisfying* (ϕ), *then either B is a C-lattice or we can find a sublattice of B consisting of a least element a^*, $c_1^* \neq c_2^* \neq c_3^* \neq c_1^*$ covering a^*, and $b = c_1^* \cap c_2^* = c_2^* \cap c_3^* = c_3^* \cap c_1^*$ covering c_1^*, c_2^*, and c_3^*.*

† *Gesammelte Werke*, 1931, vol. II, p. 255.

7. *Facts about Ideals.* Throughout, R will be understood to denote a commutative ring which has a principal unit l and satisfies the Basis Theorem. Our notation will be that of van der Waerden† except that we shall denote by (A, B) the l.c.m., and by $A \cap B$ the g.c.f., of any two given ideals A and B. This is the inverse of van der Waerden's notation.

The following are either known or immediate corollaries of known results:

(1). *The only ideals in R are R and 0 if, and only if, R is a field.*

(2). *If I is a largest ideal in R, then $0:I$ is a least ideal if and only if it is a principal ideal.*

(3). *Any ideal I covered by R is a prime ideal.*

8. *Application of Theorem* 1. On the basis of Theorem 1, it is possible to reconstruct the combinatorial theory of an important class of ideals.

By an ideal *of genus* 1 will be meant any ideal I which contains an appropriate finite product $P_1^{n_1} \cdots P_\omega^{n_\omega}$ (where P_i denotes any ideal covered by R). We shall prove the following result.

THEOREM 6. *The ideals of genus* 1 *in R are a B-lattice, which is the subdirect product of the sublattices $\mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{P}_3, \cdots$ of the primary ideals under the ideals $P_1, P_2, P_3, \cdots$ covered by R.*

That they are a lattice of which the $\mathfrak{P}_i$ are sublattices is obvious, while that they are a B-lattice follows from Theorem 27.1 of "*Subalgebras.*"

But the $\mathfrak{P}_i$ are strongly coprime, since if $Q_1, \cdots, Q_m$ satisfy the relation $Q_k \not\subset P_i$ for every k, and Q is primary under P_i, then $Q \cap (Q_1, \cdots, Q_m) = R$, being contained in no ideal covered by R. And by a theorem of E. Noether, any ideal can be expressed as the meet of a finite number of primary ideals. Theorem 6 is now merely a translation of Theorem 1 in terms of ideals.

9. *Application of Theorem* 5. It is not difficult to show from known results the following theorem.

THEOREM 7. *If R contains a largest ideal I, and another ideal $A \subset I$ for which $(A:I)/A$ is not a principal ideal, then the ideals of R are not a C-lattice.*

† *Moderne Algebra*, 1930–31; especially vol. 2, Chap 12, in which will be found the Basis and Ideal-chain Theorems.

For since l, commutativity, and the Basis Theorem are preserved under homeomorphism, we can assume $A=0$; while by (2) we can assume $(0:I)$ is not a least ideal.

By the Ideal-chain Theorem we can further choose a largest subideal $J>0$ in $0:I$, and then $x \not\in J$, $y \not\in Rx$ satisfying $y \in J$, and $w=x+y$. But a second homeomorphism permits us to assume $(Rx, Ry)=0$, yet $x \neq 0$, $y \neq 0$. This makes it obvious that $(Rx, Ry) \cap Rw \neq (Rx \cap Rw, Ry \cap Rw) \ni x$.

Conversely, suppose the ideals of R are not a C-lattice. By Theorem 5, R has a homeomorphic image R^* which contains three least ideals $A \neq B \neq C$ such that $A \cap B = B \cap C = C \cap A$.

Consider $R^*/(0:A)$; it is a field, whence, by (1), $0:A$, and similarly $0:B$ and $0:C$, are largest ideals† in R. For if $ra \neq 0$ $[a \in A, r \in R^*]$, then $ra \in A$ generates A; consequently r^{-1} exists such that $r^{-1}ra=a$ and $r^{-1}r \equiv l\ (0:A)$.

Again, if $0 \neq b \in B \subset A \cap C$, then $b=a+c$, where (since $a=0$ or $b=0$ would imply $B=C$ or $B=A$) $a \neq 0$, $c \neq 0$. And since $(A, C)=0$, $0=rb=r(a+c)=ra+rc$ implies $ra=rc=0$. Consequently $0:B \subset (0:A, 0:C)$, and $0:A=0:B=0:C=I$, where I is a largest ideal in R^*, yet, by (2), $0:I$ is not a principal ideal in R^*. Referring back to the corresponding ideals in R, we see that R does not satisfy the conclusions of Theorem 7.

We can combine Theorem 7, its converse, and Theorem 25.2 of "*Subalgebras*" in the following theorem.

THEOREM 8. *For the ideals of R to be isomorphic (with respect to l.c.m. and g.c.f.) with a system of point sets (with respect to sum and product), it is necessary and sufficient that if I is any largest ideal in R, and $A \subset I$ another ideal, then $(A:I)/A$ is a principal ideal in R/A.*

It is a corollary that the identity $A:(A:Q)=(Q \cap A)$ upon ideals is a sufficient condition for distributive combination.

HARVARD UNIVERSITY

---

† $R=0:A$ is of course excluded since $l \not\subset 0:A$.