ABSTRACT COMMUTATIVE IDEAL THEORY

R. P. DILWORTH

1. Introduction. Several years ago, M. Ward and the author [4] began a study in abstract form of the ideal theory of commutative rings. Since it was intended that the treatment should be purely ideal-theoretic, the system which was chosen for the study was a lattice with a commutative multiplication. For such multiplicative lattices, analogues of the Noether decomposition theorems for commutative rings were formulated and proved. However the theorems corresponding to the deeper results on the ideal structure of commutative rings were not obtained; the essential difficulty being the problem of formulating abstractly the notion of a principal ideal. This difficulty occurred in a mild form in treating the Noether theorem on decompositions into primary ideals. In fact, in the above mentioned paper, a weak concept of "principal element" was introduced which sufficed for the proof of the decomposition theorem into primaries. Nevertheless, the definition had serious defects and it was immediately obvious that it was not adequate for the further development of the abstract theory.

In this paper, I give a new and stronger formulation for the notion of a "principal element", and, in terms of this concept, prove an abstract version of the Krull Principal Ideal Theorem. Since there are generally many non-principal ideals of a commutative ring which are "principal elements" in the lattice of ideals, the abstract theorem represents a considerable strengthening of the classical Krull result.

It seems appropriate at this point to include a brief description of the new "principal elements" and to sketch their relationship to principal ideals.

Let L be a lattice with a multiplication and an associated residuation. The product of two lattice elements A and B will be denoted by AB and the residual, by $A:B$. An element M of L is said to be *meet principal* if

$$(A \cap B : M)M \supseteqq AM \cap B \qquad \text{all} \quad A, B \in L . \tag{1.1}$$

Similarly, M is said to be *join principal* if

$$(A \cup BM) : M \subseteqq A : M \cup B \qquad \text{all} \quad A, B \in L . \tag{1.2}$$

Finally, M is said to be *principal* if it is both meet and join principal.

Now let L be the lattice of ideals of a commutative ring R and let $M = (m)$ be a principal ideal of R. If $x \in AM \cap B$, then $x \in B$ and

Received April 20, 1961.

$x = am$ where $a \in A$. It follows that $a \in B : M$ and hence that $a \in A \cap B : M$. Thus $x = am \in (A \cap B : M)M$. According to (1.1), M is meet principal. Next let $y \in (A \cup BM) : M$. Then $ym \in A \cup BM$ and hence $ym = a + bm$ where $a \in A$ and $b \in B$. Thus $a = (y - b)m$, $y - b \in A : M$, and hence $y = (y - b) + b \in A : M \cup B$. It follows that M is also join principal. Hence every principal ideal is indeed a principal element in the lattice of ideals.

It will be shown in §7 that in polynomial rings, properties (1.1) and (1.2) in fact characterize the principal ideals. In more general rings there may be many nonprincipal ideals which are principal elements of the lattice of ideals. Thus if R is the ring of integers in an algebraic number field, then $A : B$ is the quotient $(A \cap B)/B$ and every ideal satisfies (1.1) and (1.2). We note that since distinct prime ideals of R are noncomparable, the conclusion of the Krull Principal Ideal Theorem also holds for all ideals in this ring.

2. Preliminary definitions and results.

Throughout the paper, elements of a multiplicative lattice will be denoted by latin capitals, $\cup$ and $\cap$ will denote the lattice operations and $\supseteqq$ will denote the latice inclusion relation with $\supset$ being reserved for proper inclusion. The lattices to be studied will be complete with unit element I and with null element 0.

A lattice is said to be *multiplicative* if there is defined on the lattice a commutative, associative, join distributive, multiplication. We shall also require that I be the identity element for multiplication. Such a multiplicative lattice also has a residuation satisfying the basic relations

(2.1) $\quad A \supseteqq (A : B)B$

(2.2) $\quad A \supseteqq XB$ implies $A : B \supseteqq X$.

Further important properties of the residuation and multiplication are the following

(2.3) $\quad A \supseteqq B$ if and only if $A : B = I$

(2.4) $\quad (A \cap B) : C = (A : C) \cap (B : C)$

(2.5) $\quad A : (BC) = (A : B) : C$

(2.6) $\quad A : B \supseteqq A$

(2.7) $\quad A : I = A$

(2.8) $\quad (AB) : B \supseteqq A$

(2.9) $\quad (A \cup B) : C \supseteqq (A : C) \cup (B : C)$

(2.10) $\quad (A \cap B)C \subseteqq (AC) \cap (BC)$

(2.11) $\quad (A \cap B) : B = A : B$

(2.12) $\quad A : (A \cup B) = A : B$

(2.13) $\quad A : (B \cup C) = A : \mathrm{B} \cap A : C$

(2.14) If $A \cup C = B \cup C = I$, then $(AB \cup C) = I$

(2.15) If $A \cup C = I$, then $(A \cap B) \cup C = B \cup C$

(2.16) $(A_1 \cup \cdots \cup A_n)^{k_1+\cdots+k_n} \subseteqq A_1^{k_1} \cup \cdots \cup A_n^{k_n}$.

Now let L denote a multiplicative lattice satisfying the ascending chain condition. An element $P \in L$ is *prime* if the following condition is satisfied for all $A, B \in L$

(2.17) $P \supseteqq AB$ implies $P \supseteqq A$ or $P \supseteqq B$.

The element I is trivially a prime according to this definition. However, "prime" will normally refer to prime elements distinct from I.

An element $Q \in L$ is *primary* if for all $A, B \in L$

(2.18) $Q \supseteqq AB$ implies $Q \supseteqq A$ or $Q \supseteqq B^k$ for some integer k.

Many of the results relating prime and primary ideals in a commutative ring carry over directly to multiplicative lattices. Thus if Q is a primary element of L, the join P_Q of all elements X such that $X^s \subseteqq Q$ for some integer s is a prime element containing Q. It is easily verified that P_Q is the minimal prime containing Q. Furthermore, $Q \supseteqq P_Q^k$ for some integer k. The prime P_Q is called the prime *associated* with Q and it is characterized by the properties

(2.19) $P_Q \supseteqq Q \supseteqq P_Q^k$ for some integer k

(2.20) $Q \supseteqq AB$ implies $Q \supseteqq A$ or $P_Q \supseteqq B$.

If $P_Q \not\supseteqq A$, it is easily verified that $Q : A = Q$. Also if Q_1 and Q_2 are primary elements associated with the same prime P, then $Q_1 \cap Q_2$ is likewise a primary element associated with P.

An element A is said to have a primary decomposition if there exists primaries $Q_1, \cdots, Q_m$ such that

(2.21) $A = Q_1 \cap \cdots \cap Q_m$.

If superfluous Q_i are removed and the primaries associated with the same prime are combined we obtain a reduced primary decompsition in which distinct primaries are associated with distinct primes. Such a primary decomposition is called a *normal* primary decomposition. The fundamental theorem on primary decompositions is proved exactly as in the commutative ring case and may be stated as follows:

Any two normal decompositions of an element A have the same number of components and the same set of associated primes.

Let $A = Q_1 \cap \cdots \cap Q_n$ be a normal decomposition of A and let $P_1, \cdots, P_n$ denote the associated primes. A subset $\mathfrak{S}$ of $\{P_1, \cdots, P_n\}$ is *isolated* if $P_i \in \mathfrak{S}$ implies $P_j \in \mathfrak{S}$ whenever $P_i \supseteq P_j$. The element $A_{\mathfrak{S}} = \cap \{Q_i \mid P_i \in \mathfrak{S}\}$ is called an *isolated component* of A. The fundamental result on isolated components is the following:

The element $A_{\mathfrak{S}}$ depends only upon A and $\mathfrak{S}$ and not upon the particular normal decomposition.

For let $A = Q'_1 \cap \cdots \cap Q'_n$ be a second normal decomposition and let $A'_{\mathfrak{S}} = \cap \{Q'_1 \mid P_i \in \mathfrak{S}\}$. If we set $B' = \cap \{Q'_j \mid P_j \notin \mathfrak{S}\}$, then $Q_i \supseteq A = A'_{\mathfrak{S}} \cap B' \supseteq A'_{\mathfrak{S}}B'$. Now if $P_i \in \mathfrak{S}$, then $P_i \not\supseteq B'$ since otherwise $P_i \supseteq Q'_j \supseteq P_j^k$ and hence $P_i \supseteq P_j$ so that $P_j \in \mathfrak{S}$ contrary to $P_j \notin \mathfrak{S}$. It follows that $Q_i \supseteq A'_{\mathfrak{S}}$ for all i such that $P_i \in \mathfrak{S}$. Thus $A_{\mathfrak{S}} = \cap \{Q_i \mid P_i \in \mathfrak{S}\} \supseteq A'_{\mathfrak{S}}$. Similarly $A'_{\mathfrak{S}} \supseteq A_{\mathfrak{S}}$ and hence $A_{\mathfrak{S}} = A_{\mathfrak{S}}$.

There are multiplicative lattices satisfying the ascending chain condition in which elements fail to have primary decompositions.[1] On the other hand it is well known that every element of a lattice satisfying the ascending chain condition has a decomposition into meet irreducibles. Since a meet irreducible can have a primary decomposition only if it is itself primary, it follows that the elements of L will have primary decomposition if and only if every meet irreducible element of L is primary. Suitable condition which insure that meet irreducibles will be primary involve properties of principal elements. These will be discussed in the following section.

It should be pointed out that the relationship between prime and primary elements can be developed in multiplicative lattices which are compactly generated. These include multiplicative lattices satisfying the ascending chain conditions as a very special case.

3. Noether lattices.

In §1, the notions of meet principal elements, join principal elements, and principal elements were introduced. We begin by developing some elementary properties of these elements.

LEMMA 3.1 *An element M is meet principal if and only if*

$$(A \cap B : M)M = AM \cap B \qquad \text{all } A, B \in L\,. \tag{3.1}$$

For $(A \cap B : M)M \subseteq AM \cap (B : M)M \subseteq AM \cap B$ by 2.10 and 2.1

LEMMA 3.2 *An element M is join principal if and only if*

$$(A \cup BM) : M = A : M \cup B \qquad \text{all } A, B \in L\,. \tag{3.2}$$

For $(A \cup BM) : M \supseteq A : M \cup (BM) : M \supseteq A : M \cup B$ by 2.9 and 2.8. Setting $A = I$ in 3.1 and $A = 0$ in 3.2 gives the following corollaries

[1] Ward-Dilworth [4] contains several examples.

COROLLARY 3.1. *If M is meet principal, then*

$$(B : M)M = B \cap M \qquad \text{all } B \in L . \tag{3.3}$$

COROLLARY 3.2. *If M is join principal, then*

$$(BM) : M = B \cup (0 : M) \qquad \text{all } B \in L . \tag{3.4}$$

In particular, if $M \supseteqq B$, then $(B : M)M = B$ and if $B \supseteqq 0 : M$, then $(BM) : M = B$ respectively.

LEMMA 3.3. *If M_1 and M_2 are meet principal, then M_1M_2 is meet principal.*

For

$$\begin{aligned}[A \cap B : (M_1M_2)]M_1M_2 &= [A \cap (B : M_2) : M_1]M_1M_2 \\ &= (AM_1 \cap B : M_2)M_2 = AM_1M_2 \cap B\end{aligned}$$

by (2.5) and (3.1).

LEMMA 3.4. *If M_1 and M_2 are join principal, then M_1M_2 is join principal.*

For

$$\begin{aligned}(A \cup BM_1M_2) : (M_1M_2) &= [(A \cup BM_1M_2) : M_2] : M_1 \\ &= [A : M_2 \cup BM_1] : M_1 = (A : M_2) : M_1 \cup B = A : (M_1M_2) \cup B\end{aligned}$$

by (2.5) and (3.2).

COROLLARY 3.3. *If M_1 and M_2 are principal, then M_1M_2 is principal.*

The conditions which insure that every meet irreducible is primary are formulated in the following theorem.

THEOREM 3.1. *Let L be a modular, multiplicative lattice satisfying the ascending chain condition. Furthermore let every element of L be a join of meet principal elements. Then every meet irreducible element is primary.*

Proof. Let Q be meet irreducible and let $Q \supseteqq AM$ where $Q \not\supseteqq A$ and M is meet principal. Then by (2.13) $(A \cup Q) : M \subseteqq (A \cup Q) : M^2 \subseteqq \cdots \subseteqq (A \cup Q) : M^k \subseteqq \cdots$. By the ascending chain condition there exists k such that

$$(A \cup Q) : M^k = (A \cup Q) : M^{k+1} .$$

Now let $C = (A \cup Q) \cap (M^{k+1} \cup Q)$.

Then $C : M^{k+1} = (A \cup Q) : M^{k+1} \cap (M^{k+1} \cup Q) : M^{k+1} = (A \cup Q) : M^{k+1} \cap I = (A \cup Q) : M^{k+1} = (A \cup Q) : M^k$ by (2.4).

By Lemma 3.3 M^k and M^{k+1} are meet principal and hence by (3.3) $(C : M^{k+1})M^{k+1} = C \cap M^{k+1}$ and $[(A \cup Q) : M^k]M^k = (A \cup Q) \cap M^k$. Thus by modularity we have $C = (M^{k+1} \cup Q) \cap C = Q \cup (C \cap M^{k+1}) = Q \cup (C : M^{k+1})M^{k+1} = Q \cup [(A \cup Q) : M^k]M^{k+1} = Q \cup [(A \cup Q) \cap M^k]M \subseteqq Q \cup (A \cup Q)M = Q \cup AM \cup QM \subseteqq Q \subseteqq C$.

Hence

$$Q = C = (A \cup Q) \cap (M^{k+1} \cup Q) .$$

Since Q is meet irreducible and $Q \neq A \cup Q$ we must have $Q = M^{k+1} \cup Q$ and hence $Q \supseteqq M^{k+1}$. Now let $Q \supseteqq AB$ where $Q \not\supseteqq$ A. Then B is a join of meet principal elements, say $B = M_1 \cup \cdots \cup M_r$. Thus $Q \supseteqq AM_i$ for $i = 1, \cdots, r$. Hence there exists k_i such that $Q \supseteqq M_i^{k_i}$. Let $k = k_1 + \cdots + k_r$. Then by (2.16) $Q \supseteqq B^k$ and it follows that Q is primary.

In Ward-Dilworth [4], a multiplicative lattice satisfying the ascending chain condition in which every irreducible is primary was called a "Noether lattice." Since these conditions are not sufficient for the results of commutative ideal theory we shall strengthen the definition as follows:

DEFINITION 3.1. A multiplicative lattice L is a *Noether lattice* if the following conditions are satisfied:

(1) L is modular

(2) L satisfies the accending chain condition

(3) Every element of L is a join of principal elements.

From the results of §1 we conclude *the lattice of ideals of a Noetherian ring is a Noether lattice.*

Theorem 3.4 implies that *every irreducible element of a Noether lattice is primary.* From the results of §2, it follows that *every element of a Noether lattice has a normal primary decomposition.*

Now let $A = Q_1 \cap \cdots \cap Q_n$ be a normal decomposition of A and let $\{P_1, \cdots, P_n\}$ be the associated primes. If B is an arbitrary element of L, then $\{P_i | P_i \cup B \neq I\}$ is clearly an isolated set of primes. Let A_B denote the corresponding isolated component of A. We prove now an abstract version of the intersection theorem.

THEOREM 3.2. (*Intersection Theorem*) *If A and B are elements of a Noether lattice, then* $\cap_k (A \cup B^k) = A_B$.

Proof. According to the definition of isolated components $A_B = \cap \{Q_i | P_i \cup B \neq I\}$. Let $A_B^* = \cap \{Q_j | P_j \cup B = I\}$. Now $P_j \cup B = I$

implies $P_j^k \cup B = I$ for all k by (2.14) and hence $Q_j \cup B = I$. But then

$$A_B^* = \cap \{Q_j | P_j \cup B = I\} \supseteqq \Pi \{Q_j | P_j \cup B = I\}$$

and hence $A_B^* \cup B = I$ by (2.14). From (2.14) we get $A_B^* \cup B^k = I$ all k. Hence $A \cup B^k = (A_B \cap A_B^*) \cup B^k = A_B \cup B^k$ by 2.15. Thus $A \cup B^k \supseteqq A_B$ all k and hence $\cap_k (A \cup B^k) \supseteqq A_B$.

Next let $\cap_k(A \cup B^k) \supseteqq M$ where M is principal.
Let $A \cup BM = R_1 \cap \cdots \cap R_m$ be a normal decomposition of $A \cup BM$ with associated primes $P_1', \cdots P_m'$. Then $R_i \supseteqq BM$ and hence either $R_i \supseteqq M$ or $P_i' \supseteqq B$. But if $P_i' \supseteqq B$, then $R_i \supseteqq P_i'^{k_i} \supseteqq B^{k_i}$ and hence $R_i \supseteqq A \cup B^{k_i} \supseteqq \cap_k (A \cup B^k) \supseteqq M$. In either case we get $R_i \supseteqq M$ and hence $A \cup BM = R_1 \cap \cdots \cap R_m \supseteqq M$. It follows that $A \cup BM = A \cup M$. Since M is principal we have

$$A : M \cup B = (A \cup BM) : M = (A \cup M) : M = I .$$

Thus $P_i \cup B \neq I$ implies $P_i \not\supseteqq A : M$. Since $Q_i \supseteqq A \supseteqq (A : M)M$ it follows that $Q_i \supseteqq M$ for all i such that $P_i \cup B \neq I$. Hence $A_B = \cap \{Q_i | P_i \cup B \neq I\} \supseteqq M$.
Since L is a Noether lattice, $\cap_k (A \cup B^k)$ is a join of principal elements. Thus

$$A_B \supseteqq \bigcap_k (A \cup B^k)$$

and the proof of the theorem is complete

Setting $A = 0$ in Theorem 3.2 we get

COROLLARY 3.1. *If B is an element of a Noether lattice L, then*

$$\cap B^k = 0_B .$$

If $A \neq I$ is an element of a Noether lattice, then there exists a maximal element $P \neq I$ such that $P \supseteqq A$. By (2.14) and (2.17) such an element is prime and clearly is a maximal prime of L.

DEFINITION 3.2. A Noether lattice L is *local* if it contains precisely one maximal prime.

Now suppose that L is local with the unique maximal prime P_0. If $P_i \neq I$ and $B \neq I$, then $P_0 \supseteqq P_i \cup B$ and hence $P_i \cup B \neq I$. Thus $A_B = \cap \{Q_i | P_i \cup B \neq I\} = A$. Accordingly we get

COROLLARY 3.2. *If L is a local Noether lattice and $B \neq I$ is an element of L, then for each $A \in L$*

$$\bigcap_k (A \cup B^k) = A .$$

Setting $A = 0$, we have

COROLLARY 3.3. *If $B \neq I$ is an element of a local Noether lattice, then*

$$\bigcap_k B^k = 0 .$$

4. Quotient lattices. If L is a Noether lattice and $D \in L$, then $L/D = \{A \in L \mid A \supseteqq D\}$ is clearly a sublattice of L. However, L/D need not be closed with respect to multiplication. We make L/D into a multiplicative lattice by defining

$$A \circ B = AB \cup D .$$

This multiplication is easily seen to be commutative, associative, distributive with respect to join, and has I as an identity element. Thus with this multiplication L/D is a multiplicative lattice.

Since $A : B \supseteqq A$, it follows that L/D is closed with respect to residuation. This residuation is also the residuation associated with $A \circ B$ since

$$A \supseteqq X \circ B \text{ if and only if } A \supseteqq XB .$$

LEMMA 4.1. *If L is a Noether lattice, then L/D is a Noether lattice. Furthermore if M is a principal element of L, then $M \cup D$ is a principal element of L/D.*

For if L is modular and satisfies the ascending chain condition, then clearly L/D is modular and satisfies the ascending chain condition.

Now let M be a principal element of L and let $A, B \in L/D$. Then

$$\begin{aligned}[A \cup B\circ(M \cup D)] : (M \cup D) &= (A \cup BM \cup D) : (M \cup D) \\ &= (A \cup BM \cup D) : M = (A \cup BM) : M \\ &= A : M \cup B = A : (M \cup D) \cup B\end{aligned}$$

and $M \cup D$ is thus join principal. On the other hand

$$\begin{aligned}&[A : (M \cup D) \cap B]\circ(M \cup D) = (A : M \cap B)\circ(M \cup D) \\ &\quad = (A : M \cap B)(M \cup D) \cup D \\ &\quad = (A : M \cap B)M \cup (A : M \cap B)D \cup D = (A : M \cap B)M \cup D \\ &\quad = (A \cap BM) \cup D = A \cap (BM \cup D) \\ &\quad = (A \cap (BM \cup BD) \cup D) = A \cap B\circ(M \cup D) .\end{aligned}$$

and $M \cup D$ is thus meet principal. Note that modularity is required in the sixth step of this argument. Now if $A \in L/D$, then $A = A \cup D = M_1 \cup \cdots \cup M_k \cup D = (M_1 \cup D) \cup \cdots \cup (M_k \cup D)$ and hence every element of L/D is a join of principal elements. Thus L/D is a Noether lattice.

The next lemma shows that the arithmetical properties of L are preserved in L/D.

LEMMA 4.2. *An element is prime or primary in L/D if and only if it is prime or primary in L.*

Let $A, B, C \in L/D$. Then $A \supseteq B \circ C$ if and only if $A \supseteq BC$. Hence A is prime or primary if and only if it is prime or primary in L.

COROLLARY 4.1. *If L is a local Noether lattice, and $D \neq I$, then L/D is a local Noether lattice.*

5. Congruence lattices. Congruence relations provide a second method for constructing new Noether lattices from a given Noether lattice. This construction is the abstract version of the construction of the generalized ring of quotients introduced by Chevalley [1]. Let L be a Noether lattice and let D be an arbitrary element of L. If $P_1, \cdots, P_n$ are the primes associated with a normal decompsition of A, then $\{P_i \mid D \supseteq P_i\}$ is an isolated set of primes and hence determines an isolated component A_D of A. For a given normal decomposition $A = Q_1 \cap \cdots \cap Q_n$ we have $A_D = \cap \{Q_i \mid D \supseteq P_i\}$. We will let A'_D denote $\{Q_j \mid D \not\supseteq P_j\}$ so that $A = A_D \cap A'_D$. We define $A \equiv B(D)$ if and only if $A_D = B_D$.

LEMMA 5.1. *If $A \supseteq B$, $A_D \supseteq B_D$.*

For let $A = Q_1 \cap \cdots \cap Q_m$ be a normal decomposition of A and let $P_1, \cdots, P_m$ be the associated primes. If $D \supseteq P_i$, then $Q_i \supseteq A \supseteq B \supseteq B_D \cap B'_D$. If $P_i \supseteq B'_D$, then $P_i \supseteq P'_j$ where $D \not\supseteq P'_j$ contrary to $D \supseteq P_i$. Hence $P_i \not\supseteq B'_D$ and thus $Q_i \supseteq B_D$. It follows that $A_D = \cap \{Q_i \mid D \supseteq P_i\} \supseteq B_D$.

LEMMA 5.2. *If $A \equiv B(D)$,* then *$A \cap C \equiv B \cap C(D)$.*

For let $A \cap C = Q_1 \cap \cdots \cap Q_n$ be a normal decomposition of $A \cap C$ with associated primes $P_1, \cdots P_n$. Then if $D \supseteq P_i$ we have $Q_i \supseteq A \cap C = A_D \cap C \cap A'_D$ and $P_i \not\supseteq A'_D$. Thus $Q_i \supseteq A_D \cap C = B_D \cap C \supseteq B \cap C$. Thus $(A \cap C)_D = \cap \{Q_i \mid D \supseteq P_i\} \supseteq B \cap C$. But then $(A \cap C)_D = ((A \cap C)_D)_D \supseteq (B \cap C)_D$ by Lemma 5.1. Similarly $(B \cap C)_D \supseteq (A \cap C)_D$ and thus $(A \cap C)_D = (B \cap C)_D$. It follows that $A \cap C \equiv B \cap C(D)$.

LEMMA 5.2. *If $A \equiv B(D)$, then $A \cup C \equiv B \cup C(D)$.*

For let $A \cup C = Q_1 \cap \cdots \cap Q_n$ be a normal decomposition of $A \cup C$ with associated primes $P_1, \cdots, P_n$. Then if $D \supseteq P_i$ we have $Q_i \supseteq A_D \cap A'_D$ and $Q_i \supseteq C$. Since $P_i \not\supseteq A'_D$ we have $Q_i \supseteq A_D$. Thus $Q_i \supseteq B_D \supseteq B$ and this $Q_i \supseteq B \cup C$. But then $(A \cup C)_D = \cap \{Q_i \mid D \supseteq P_i\} \supseteq B \cup C$ and hence $(A \cup C)_D \supseteq (B \cup C)_D$ by Lemma 5.1. Similarly $(B \cup C)_D \supseteq (A \cup C)_D$ and hence $A \cup C \equiv B \cup C(D)$.

LEMMA 5.3. *If* $A \equiv B(D)$, *then* $AC \equiv BC(D)$.

For let $AC = Q_1 \cap \cdots \cap Q_n$ be a normal decomposition of AC with associated primes $P_1, \cdots, P_n$. Then if $D \supseteq P_i$ we have $Q_i \supseteq AC = (A_D \cap A'_D)C \supseteq A_D C A'_D$ where $P_i \not\supseteq A'_D$. Thus $Q_i \supseteq A_D C = B_D C \supseteq BC$. It follows that $(AC)_D \supseteq BC$ and hence by Lemma 5.1 that $(AC)_D \supseteq (BC)_D$. Similarly $(BC)_D \supseteq (AC)_D$ and hence the conclusion of the lemma follows.

LEMMA 5.4. *If* $A \equiv B(D)$, *then* $A : C \equiv B : C(D)$ *and* $C : A \equiv C : B(D)$.

For let $X : Y = Q_1 \cap \cdots \cap Q_n$ be a normal decomposition of $X : Y$ with associated primes $P_1, \cdots, P_n$. Then if $D \supseteq P_i$ we have $Q_i \supseteq X : Y = (X_D \cap X'_D) : Y = (X_D : Y) \cap (X'_D : Y) \supseteq (X_D : Y)(X'_D : Y)$. Now $P_i \not\supseteq X'_D : Y$ since otherwise $P_i \supseteq X'_D : Y \supseteq X'_D$. Thus $Q_i \supseteq X_D : Y \supseteq X_D : Y_D$ since $Y_D \supseteq Y$. Hence $(X : Y)_D = \cap \{Q_i \mid D \supseteq P_i\} \supseteq X_D : Y_D$.

On the other hand, $X \supseteq (X : Y)Y$ and hence

$$X_D \supseteq [(X : Y)Y]_D = (X : Y)_D Y_D \text{ by Lemma 5.1 and 5.3 .}$$

Hence $X_D : Y_D \supseteq (X : Y)_D$ and thus $(X : Y)_D = X_D : Y_D$ by the result of the previous paragraph.

Now if $A \equiv B(D)$, then $(A : C)_D = A_D : C_D = B_D : C_D = (B : C)_D$ and thus $A : C = B : C(D)$. Similarly $C : A \equiv C : B(D)$.

Lemma 5.1–5.4 show that congruence mod D is a congruence relation on L preserving meet, join, multiplication, and residuation. In view of the fact that principal elements are defined in terms of equations involving meet, join, multiplication, and residuation it follows that the congruence class of a principal element is principal in the lattice of congruence classes.

Now let L_D denote the multiplicative lattice of congruence classes. Then we have

THEOREM 5.1. *If L is a Noether lattice, then L_D is a Noether lattice.*

The arithmetical properties of L_D may be described as follows:

THEOREM 5.2. *The primes and primaries of L_D are precisely the congruence classes determined by the primes and primaries of L. The proper prime elements of L_D are the congruence classes determined by primes P such that $D \supseteq P$.*

Proof. Let the congruence class $\{C\}$ be a prime in L_D. Now $C \supseteq P_1^{k_1} \cdots P_n^{k_n}$ where $P_1, \cdots, P_n$ are primes of L such that $P_i \supseteq C$. But then $\{C\} \supseteq \{P_1\}^{k_1} \cdots \{P_n\}^{k_n}$ and hence $\{C\} \supseteq \{P_i\} \supseteq \{C\}$ for since i. Thus $\{C\} = \{P_i\}$ where P_i is a prime of L. Conversely, if P is a prime of L, then, by definition, $P_D = P$ or $P_D = I$ according as $D \supseteq P$ or $D \not\supseteq P$. Hence $\{P\} \supseteq \{A\}\{B\}$ implies $P_D \supseteq A_D B_D$ and hence $P_D \supseteq A_D$ or

$P_D \supseteqq B_D$ which implies $\{P\} \supseteqq \{A\}$ or $\{P\} \supseteqq \{B\}$. Thus the primes of L_D have the form $\{P\}$ where P is a prime of L and $\{P\}$ is proper if and only if $D \supseteqq P$.

Next let $\{C\}$ be a primary element of L_D associated with the prime $\{P\}$. Now $C_D = Q_1 \cap \cdots \cap Q_r$ when $D \supseteqq P_i$ and P_i is the prime associated with Q_i. We may suppose that $\{C\} \neq \{I\}$ and thus that $D \supseteqq P$. Now $\{C\} \supseteqq \{P\}^k$ for some k. Hence $C_D \supseteqq P_D^k = P^k$. But then $P_i \supseteqq P$ for all i. Since $P \supseteqq C_D$ we have $P \supseteqq P_j$ for some j and hence $P = P_j$. On the other hand $P_1, \cdots, P_r$ are distinct and thus $P \not\supseteqq P_i$ for $i \neq j$. Since $\{C\} \supseteqq \{Q_1\} \cdots \{Q_r\}$ and $\{P\} \not\supseteqq \{Q_i\}$ for $i \neq j$. We have $\{C\} \supseteqq \{Q_j\}$ since $\{C\}$ is primary in L_C. But then $\{C\} = \{Q_j\}$ where Q_j is a primary of L. Conversely if Q is a primary element of L, then, by definition, $Q_D = Q$ or $Q_D = I$ according as $D \supseteqq P_Q$ or $D \not\supseteqq P_Q$. Hence $\{Q\} \supseteqq \{A\}\{B\}$ implies $\{Q\} \supseteqq \{A\}$ or $\{P\} \supseteqq \{B\}$ and $\{Q\}$ is a primary element of L_D. This completes the proof of the theorem.

It should be noted that distinct primes contained in D determine distinct congruence classes.

THEOREM 5.3. *If P is a proper prime of L, then L_P is a local Noether lattice.*

Proof. For if $\{P'\}$ is a proper prime of L_P, then $P \supseteqq P'$ and hence $\{P\} \supseteqq \{P'\}$. On the other hand $\{P\}$ is a proper prime of L_P. Thus $\{P\}$ is the unique maximal proper prime of L_P.

6. The principal element theorem. The critical steps in the proof of the principal element theorem will depend upon the finite dimensionality of certain quotient lattices. The finite dimensionality rests in turn upon the following theorem on modular lattices.

THEOREM 6.1. *Let S be a subset of a modular lattice L which generates L under finite joins. Then if S satisfies the descending chain condition, L also satisfies the descending chain condition.*

We begin by proving two lemmas on quotient lattices in a modular lattice.

LEMMA 6.1. *Let L be a modular lattice. If a/b and b/c are quotient lattices satisfying the descending chain condition, then a/c satisfies the descending chain condition.*

For let $x_1 \geqq x_2 \geqq \cdots \geqq x_n \geqq \cdots$ be a descending chain in a/c. Then $x_1 \cup b \geqq x_2 \cup b \geqq \cdots \geqq x_n \cup b \geqq \cdots$ and $x_1 \cap b \geqq x_2 \cap b \geqq \cdots \geqq x_n \cap b \geqq \cdots$ are descending chains in a/b and b/c respectively. Hence there exists an integer k such that $x_n \cup b = x_k \cup b$ and $x_n \cap b = x_k \cap b$ all $n \geqq k$.

Since $x_k \geqq x_n$ all $n \geqq k$ it follows from the modular law that $x_k = x_n$ all $n \geqq k$ and hence a/c satisfies the descending chain condition.

LEMMA 6.2. *Let L be a modular lattice. If a/b and c/d satisfy the descending chain condition, then $a \cup c/b \cup d$ and $a \cap c/b \cap d$ satisfy the descending chain condition.*

For $a/a \cap (b \cup d)$ is a subquotient of a/b and hence satisfies the descending chain condition. But $a/a \cap (b \cup d)$ is isomorphic to $a \cup d/b \cup d$ and hence $a \cup d/b \cup d$ satisfies the descending chain condition. A similar argument shows that $a \cup c/a \cup d$ satisfies the descending chain condition. But then $a \cup c/b \cup d$ satisfies the descending chain condition by Lemma 6.1. A dual proof shows that $a \cap c/b \cap d$ likewise satisfies the descending chain condition.

Repeated application of Lemma 6.2 gives the following corollary.

COROLLARY 6.1. *Let L be a modular lattice. If $a_1/b, \cdots, a_n/b$ satisfy the descending chain condition, then $(a_1 \cup \cdots \cup a_n)/b$ satisfies the descending chain condition.*

We now give the proof of the theorem.

Proof of Theorem 6.1. If s_1 and s_2 are elements of S, then $s_1 \cap s_2$ is a join of elements of S. Hence there exists $s_3 \in S$ such that $s_1 \geqq s_3$ and $s_2 \geqq s_3$. Thus S is a directed set and hence has a null element z by the descending chain condition. z is clearly the null element of L. We shall show first that the quotient lattices s/z satisfy the descending chain condition by making an induction upon the elements of S. Clearly z/z satisfies the descending chain condition. Let us suppose that s/z satisfies the descending chain condition for all $s < s_0$. If s_0/z does not satisfy the descending chain condition, there exists an infinite descending chain

$$a_0 > a_1 > \cdots > a_n > \cdots$$

in s_0/z. Then $s_0 \geqq a_0 > a_1$ and $a_1 = s_1 \cup \cdots \cup s_n$. But then s_i/z satisfies the descending chain condition by the induction assumption and hence $a_1/z = (s_1 \cup \cdots \cup s_n)/z$ satisfies the descending chain condition by Corollary 6.1. But $a_1 > \cdots > a_n > \cdots$ is an infinite descending chain in a_1/z. Hence s_0/z satisfies the descending chain condition. Since S itself satisfies the descending chain condition it follows by induction that s/z satisfies the descending chain condition for all $s \in S$. Now let $a \in L$ and let $a = s_1 \cup \cdots \cup s_m$. Since s_i/z satisfies the descending chain condition for each i, it follows from Corollary 6.1 that a/z satisfies the descending chain condition and hence that L itself satisfies the descending chain condition. This completes the proof of the theorem.

The following theorem describes the finite dimensionality properties of local Noether lattices.

THEOREM 6.2. *Let L be a local Noether lattice with maximal prime P. Then L/P^k is finite dimensional.*

Proof. The elements $P^k \cup M$ where M is principal generate L/P^k under finite joins. Hence by Theorem 6.1 it will suffice to show that these elements satisfy the descending chain condition. Let

$$P^k \cup M_1 \supset P^k \cup M_2 \supset \cdots \supset P^k \cup M_n \cdots$$

We may clearly assume that $P^k \cup M_1 \neq I$. Since L has exactly one maximal prime element P it follows that $P \supseteqq P^k \cup M_1 \supseteqq M_1$. Now $(P^k \cup M_{r+1}) : M_r \neq I$ since otherwise $M_r = [(P^k \cup M_{r+1}) : M_r]M_r = (P^k \cup M_{r+1}) \cap M_r$ by Corollary 3.1 and hence $P^k \cup M_{r+1} \supseteqq M_r$ which implies $P^k \cup M_{r+1} \supseteqq P^k \cup M_r$ contrary to $P^k \cup M_r \supset P^k \cup M_{r+1}$. Thus

$$P \supseteqq (P^k \cup M_{r+1}) : M_r \text{ for all } r\ .$$

Now $P \supseteqq M_1$. Suppose that $P^r \supseteqq M_r$ where $r < k$. Then

$$\begin{aligned} P^{r+1} \supseteqq [(P^k \cup M_{r+1}) : M_r]P^r &\supseteqq [(P^k \cup M_{r+1}) : M_r]M_r \\ &= (P^k \cup M_{r+1}) \cap M_r\ . \end{aligned}$$

Thus $P^{r+1} \supseteqq P^k \cup [(P^k \cup M_{r+1}) \cap M_r] = (P^k \cup M_{r+1}) \cap (P^k \cup M_r) = P^k \cup M_{r+1} \supseteqq M_{r+1}$ by the modular law. Hence by induction we get

$$P^k \supseteqq M_k\ .$$

Thus $P^k = P^k \cup M_k \supset P^k \cup M_{k+1} \supseteqq P^k$ which is impossible. It follows that the elements $P^k \cup M$ satisfy the descending chain condition and hence L/P^k is finite dimensional.

A lemma on lattice isomorphism will be needed in the proof of the main theorem.

LEMMA 6.3. *Let L be a Noether lattice in which 0 is a prime. Then if M is a nonzero principal element the quotient lattice AM/BM is lattice isomorphic to A/B.*

For if 0 is a prime, then $0 \supseteqq (0 : X)X$ where $X \neq 0$ implies $0 \supseteqq 0 : X$. Hence $0 : X = 0$ whenever $X \neq 0$. But then $(XM) : M = (0 \cup XM) : M = 0 : M \cup X = X$. Now the mapping $X \to XM$ maps A/B into AM/BM. It is order preserving since $X \supseteqq Y$ implies $XM \supseteqq YM$. It is 1-1 since $XM = YM$ implies $X = (XM) : M = (YM) : M = Y$. Finally if $V \in AM/BM$, then $AM \supseteqq V$ and hence $V = V \cap AM = (V : M \cap A)M$ since M is principal. But $A \supseteqq A \cap V : M \supseteqq A \cap (BM) : M \supseteqq A \cap B = B$ and hence

$X = A \cap V : M$ maps onto V. Thus $X \to XM$ is a 1-1 order preserving map of A/B onto AM/BM and hence A/B and AM/BM are lattice isomorphic:

In formulating the proof of the Principal Element Theorem, we will make use of a modification of an argument due to D. Rees [3].

THEOREM 6.3. *Let L be a local Noether lattice in which 0 is a prime. Let P be the maximal prime of L. Then if the principal element M is primary with associated prime P, P is the only non zero prime of L.*

Proof. Let P' be a nonzero prime of L. Then $P' \supseteqq N$ where N is a nonzero principal element of L. Now by (2.13)

$$N : M \subseteqq N : M^2 \subseteqq \cdots \subseteqq N : M^n \subseteqq \cdots .$$

Since the ascending chain condition holds in L, it follows that $N : M^k = N : M^{k+1}$ for some k. But then

$$N \cap M^{k+1} = (N : M^{k+1})M^{k+1} = (N : M^k)M^k M = (N \cap M^k)M .$$

Then if $d(A/B)$ denotes the dimension of the quotient A/B we have

$$\begin{aligned} d((N \cup M^{k+1})/M^{k+1}) &= d(N/(N \cap M^{k+1})) \\ &= d(N/(N \cap M^k)M) \\ &= d(N/NM) + d(NM/(N \cap M^k)M) \\ &= d(I/M) + d(N/(N \cap M^k)) \\ &= d(M^k/M^{k+1}) + d((N \cup M^k)/M^k) \\ &= d((N \cup M^k)/M^{k+1}) \end{aligned}$$

making use of modularity and Lemma 6.3. Note that all of the quotients are finite dimensional since $M \supseteqq P^l$ for some l and hence $M^{k+1} \supseteqq P^{(k+1)l}$. But $L/P^{(k+1)l}$ is finite dimensional by Theorem 6.2. Since $N \cup M^k \supseteqq N \cup M^{k+1}$ it follows from the equality of the dimension that $N \cup M^k = N \cup M^{k+1}$.

Then

$$\begin{aligned} M^k = M^k \cap (N \cup M^k) = M^k \cap (N \cup M^{k+1}) &= (M^k \cap N) \cup M^{k+1} \\ &= (N : M^k)M^k \cup M^{k+1} = (N : M^k \cup M)M^k . \end{aligned}$$

Hence $I = M^k : M^k = [(N : M^k \cup M)M^k] : M^k = N : M^k \cup M$. Now $P \not\supseteqq N : M^k$ since otherwise $P \supseteqq N : M^k \cup M = I$. Since L is local with maximal prime P it follows that $N : M^k = I$ and hence $N \supseteqq M^k$. But then

$$P' \supseteqq N \supseteqq M^k \supseteqq P^{kl} .$$

Thus $P' \supseteqq P$ and since P is maximal we have $P' = P$. This completes the proof of the theorem.

DEFINITION 6.1. Let P be a prime element of a Noether lattice L. The least upper bound of the length of chains $P \supset P_1 \supset P_2 \supset \cdots \supset P_k$ where the P_i are primes of L is called the *rank* of P.

The abstract version of the Krull Principal Ideal Theorem (Krull [2]) is formulated as follows:

THEOREM 6.4. (*Principal Element Theorem*) *Let P be a minimal prime containing the principal element M of a Noether lattice. Then the rank of P is at most one.*

Proof. Let L denote the Noether lattice. Without any loss of generality we may suppose that L is local and that P is the maximal prime of L. For L_P is a local Noether lattice in which the maximal prime is the congruence class of P. By Theorem 5.2, the rank of the congruence class of P in L_P is the same as the rank of P in L. But if L is a local Noether lattice and P is the maximal prime of L, then M is primary with P as the associated prime. For let P_i be a prime associated with a normal decomposition of M. Then $P \supseteqq P_i$ since P is maximal. But since P is minimal over M we must have $P = P_i$ and hence M is primary associated with P.

Now let $P \supset P_1 \supseteqq P_2$. Then L/P_2 is a local Noether lattice with maximal prime P. The zero element of L/P_2 is P_2 which is prime by Lemma 4.2. Also by Lemma 4.2, the principal element $M \cup P_2$ of L/P_2 is primary with P as associated prime. Hence by Theorem 6.3, P is the only nonzero prime of L/P_2. But by Lemma 4.2, P_1 is a prime of L/P_2 which is distinct from P. Thus $P_1 = P_2$ and the rank of P is at most one.

We will conclude this section by proving the theorem which extends the result of Theorem 6.4 to nonprincipal elements. A preliminary lemma is required.

LEMMA 6.4. *Let L be a Noether lattice and let $P = P_0 \supset P_1 \supset \cdots \supset P_{r-1} \supset P_r$ be a chain of prime elements of L. If M is a principal element of L such that $P \supseteqq M$, then there exists a chain of prime elements $P = P_0^* \supset P_1^* \supset \cdots P_{r-1}^* \supset P_r$ such that $P_{r-1}^* \supseteqq M$.*

For let us set $P_0^* = P_0 = P$. If $P_1 \supseteqq M$ we set $P_1^* = P_1$, otherwise we let P_1^* be a minimal prime such that $P \supseteqq P_1^* \supseteqq M \cup P_2$. Then P_1^* is a minimal prime containing the principal element $M \cup P_2$ of L/P_2. Hence by Theorem 6.4 we conclude that $P \neq P_1^*$ since P is of rank two in L/P_2. Also since $P_1 \not\supseteqq M$ we have $P_2 \not\supseteqq M$ and hence $P_1^* \neq P_2$. Thus

$P = P_0^* \supset P_1^* \supset P_2$ and $P_1^* \supseteqq M$. Repeating this argument $r-1$ times gives the chain $P = P_0 \supset P_1^* \supset \cdots \supset P_{r-1}^* \supset P_r$ with $P_{r-1}^* \supseteqq M$.

THEOREM 6.5. *Let L be a Noether lattice and let P be a minimal prime containing $M_1 \cup \cdots \cup M_k$ where each M_i is principal. Then the rank of P is at most k.*

Proof. Let $P = P_0 \supset P_1 \supset \cdots \supset P_{r-1} \supset P_r$ be an arbitrary chain of primes beginning with P. Then $P \supseteqq M_k$ and hence by Lemma 6.4 there exists a chain $P = P_0^* \supset P_1^* \supset \cdots \supset P_{r-1}^* \supset P_r$ such that $P_{r-1}^* \supseteqq M_k$. Now P is a minimal prime containing $(M_1 \cup M_k) \cup \cdots \cup (M_{k-1} \cup M_k)$ where each $M_i \cup M_k$ is principal in L/M_k. Since $P = P_0^* \supset \cdots \supset P_{r-1}^*$ is a prime chain in L/M_k we may suppose by induction that $r - 1 \leqq k - 1$ and hence conclude that $r \leqq k$. This completes the proof of the theorem.

7. Polynomial ideals. In this section it will be shown that the principal elements of the lattice of ideals of a unique factorization integral domain are precisely the principal ideals. In particular, this result holds for ideals in a polynomial ring.

THEOREM 7.1. *Let R be a unique factorization integral domain. Then every principal element in the lattice of ideals of R is a principal ideal.*

Proof. Let $M = (m_1, \cdots, m_k)$ be a principal element in the lattice of ideals of R. Then $M \supseteqq (m_i)$ and hence $(m_i) = (m_i) \cap M = ((m_i) : M)M = X_iM$ where $X_i = (m_i) : M$. Then there exist elements $x_{i1}, \cdots, x_{ik}$ in X_i such that

$$m_i = x_{i1}m_1 + \cdots + X_{ik}m_k \qquad i = 1, \cdots, k .$$

Let

$$\Delta = \begin{vmatrix} 1 - x_{11} & -x_{12} & \cdots & -x_{1k} \\ -x_{21} & 1 - x_{22} & \cdots & -x_{2k} \\ \cdots & \cdots & \cdots & \cdots \\ -x_{k1} & -x_{k2} & \cdots & 1 - x_{kk} \end{vmatrix}$$

Then $\Delta m_i = 0$ for $i = 1, \cdots, k$ and hence $\Delta = 0$ since R is an integral domain. But $\Delta = 1 - x$ where $x \in X_1 \cup \cdots \cup X_x$. Hence $X_1 \cup \cdots \cup X_k = (1)$ and thus there exist elements $x_i \in X_i$ such that

$$x_1 + \cdots + x_n = 1 .$$

Since $(m_i) = X_iM$ there exist elements r_{ij} such that

$$x_im_j = r_{ij}m_i .$$

Let b be the g. c. d. of $m_1, \cdots, m_k$. Then since R is a unique factorization domain it follows that x_i is a multiple of m_i/d. Thus $dx_i = y_i m_i$. Hence

$$d = dx_1 + \cdots + dx_k = y_1 m_1 + \cdots + y_k m_k \in M .$$

On the other hand it is clear that $M \subseteqq (d)$. Hence $M = (d)$ and it follows that M is a principal ideal.

It should be noted that if L is a Noether lattice which satisfies the cancellation law for nonzero elements and in which every element has a unique factorization into primes (for example, the lattice of ideals of the ring of integers in an algebraic number field), then $A : B = (A \cap B)/B$ and hence 1.1 and 1.2 hold identically in L. Thus every element of L is principal. R. S. Pierce notes that the converse is also true. *If L is a Noether lattice in which 0 is prime and in which every element is principal, then the cancellation law holds in L and every element of L has a unique decomposition into primes.* The cancellation law follows from Lemma 6.3 and the unique decomposition into primes can be deduced from Corollary 3.1.

8. Distributive lattices.

Let L be a distributive lattice satisfying the ascending chain condition and with a null element 0. Then if the meet operation is taken as the multiplication it is well known (Ward [5]) that L is a multiplicative lattice with residuation. Since L is modular and satisfies the ascending chain condition, L will be a Noether lattice if and only if the principal elements of L generate L under finite joins.

LEMMA 8.1. *M is a principal element of L if and only if M has a complement in L.*

For let M be principal. Then $0 \supseteqq (0 : M) \cap M$ and hence $(0 : M) \cap M = 0$. On the other hand, $0 : M \cup M = [0 \cup (M \cap M] : M = M : M = I$ and hence $0 : M$ is a complement of M. Conversely, suppose that M is an element with a complement M'. It is easily verified that $X : M = X \cup M'$. Hence

$$[A \cup (B \cap M)] : M = A \cup (B \cap M) \cup M' = A \cup M' \cup B = A : M \cup B$$

$$[A \cap (B : M)] \cap M = [A \cap (B \cup M')] \cap M = (A \cap M) \cap B$$

and M is principal. The proof of the lemma is thus complete.

Now the complemented elements of a distribution lattice are closed under meet and join and form a Boolean algebra. Thus we get

THEOREM 8.1. *A distributive lattice is a Noether lattice if and only if it is a finite Boolean algebra.*

It should be noted that the prime elements of a Boolean algebra are the elements covered by the unit element. Any two such elements are non comparable and hence the rank of every proper prime is zero.

REFERENCES

1. C. Chevalley, *On the notion of the ring of quotients of a prime ideal*, Bull. Amer. Math. Soc., **50** (1944), 93-97.
2. W. Krull, *Dimensionstheorie in Stellenringe J. reine angew*, Math. **179** (1938), 204-226.
3. D. Rees, *Two classical theorems of ideal theory*, Proc. Camb. Phil. Soc., **52** (1956), 155-157.
4. M. Ward and R. P. Dilworth, *Residuated lattices*, Trans. Amer. Math. Soc., **45** (1939), 335-354.
5. M. Ward, *Residuated distributive lattices*, Duke Math. Journal **6** (1940), 641-651.

CALIFORNIA INSTITUTE OF TECHNOLOGY