MATH. SCAND. 1 (1953)

ON THE IDEAL THEORY OF COMMUTATIVE SEMI-GROUPS

KARL EGIL AUBERT

Introduction. It is wellknown from the ideal theory of Prüfer and Lorenzen ([9], [7], and [8]) that there may be defined various fruitful ideal concepts in the theory of rings and semi-groups. In the present paper we shall give some results on the simplest one of these ideal concepts—the so-called s-ideals.

The main contents of the paper are as follows. In the first section we state some basic definitions together with a simple and well-known result on the structure of the lattice of all s-ideals of a commutative semi-group. Next we make some remarks on the ascending chain condition for s-ideals. In the following section we characterize those semi-groups which satisfy both the ascending and the descending chain conditions for s-ideals. It turns out that these semi-groups are those which contain only a finite number of mutually non-associate elements. Among the semi-groups which satisfy the ascending chain condition for s-ideals those in which every s-ideal is principal are then characterized by the fact that their lattice of s-ideals is always a chain. The next section deals with the problem of giving basis representations for s-ideals. This discussion leads for instance to the result that the only semi-groups which possess a basis in a certain strict sense are the groups. The theory of s-Noetherian semi-groups is treated very briefly in section six. Since that theory may be included in the general theory of residuated lattices as developed by Ward and Dilworth ([14] and [12]) most of the results of that section are stated without proofs. We have, however, included a proof of the fundamental fact that an s-irreducible s-ideal in an s-Noetherian semi-group is primary because our direct proof of this theorem is somewhat simpler than the proof of the general lattice theorem ([14], p. 349, Theorem 11.2) from which it may be derived. In the two final sections we make various remarks on s-ideals in ring- and valuation theory.

Many of the results of the present paper have immediate generalizations to r-ideals in the sense of Prüfer-Lorenzen. There are also, however,

Received March 27, 1953.

various points which, in the case of general r-ideals, require a closer examination. But we shall not enter upon these questions here.

1. s-ideals in commutative semi-groups. By a semi-group is usually understood a set in which there is defined an associative binary operation. We shall in the following deal exclusively with *commutative* semi-groups S having an *identity* e satisfying $ae = a$ for all $a \in S$. In the present paper we shall therefore use the terms 'semi-group' and 'commutative semi-group (with an identity)' as synonyms. If the cancellation law $ab = ac \rightarrow b = c$ holds in S we shall say that S is a *regular* semi-group. Most of our results concern general (non-regular) semi-groups so that these results will also apply to rings having divisors of zero. We say that a *divides* b, and write $a|b$ if there exists an element $c \in S$ such that $ac = b$, (a is a *divisor* of b, b is a *multiple* of a). If $a|b$ and $b|a$ we say that a and b are *associate*, and write $a \sim b$. A divisor of the identity element e is called a *unit*. The set of all units in S is a group. If S is regular, two elements are associate if and only if they differ only by a unit factor. By the *product* AB of two subsets A, B of S we shall mean the subset of S consisting of all products ab with $a \in A$ and $b \in B$. An *s-ideal* in S (small German letters will always denote ideals) is a subset $\mathfrak{a}$ of S such that $S\mathfrak{a} \subseteq \mathfrak{a}$. In the case that S does not contain a *zero element*, i. e. an element 0 satisfying $a0 = 0$ for every $a \in S$ we shall agree to consider the void set as an s-ideal. With this convention it is readily seen that the set of s-ideals of S forms a lattice under set-inclusion and that this lattice is a sublattice of the lattice (Boolean algebra) of all subsets of S. This lattice consisting of all s-ideals in S, will always be denoted by $\mathcal{S}$. Since further the product of two s-ideals is again an s-ideal and this product is completely distributive with respect to union we conclude as in [13]:

THEOREM 1. *The set of all s-ideals in a commutative semi-group form a completely distributive and residuated lattice under set-inclusion and multiplication.*

In the following the usual (Dedekindian) ideals in commutative rings are called *d-ideals*. We note the difference between the above theorem and the situation for d-ideals in rings. The lattice of all d-ideals in a commutative ring is modular but in general not distributive. The fact that the lattice $\mathcal{S}$ is distributive leads to a stronger unicity statement concerning irreducible decompositions, since the irredundant intersection representation by irreducibles is unique in a distributive lattice, but in general not in a modular one. (We shall return to this in sections 6 and 7.) As usual we call an intersection representation $a = a_1 \cap a_2 \cap \ldots \cap a_n$ *ir-*

redundant if we never have $a_1 \cap \ldots \cap a_{i-1} \cap a_{i+1} \cap \ldots a_n \subseteq a_i$ for $i = 1, 2, \ldots n$. An irredundant union representation is defined in a dual way.

We define a semi-group S as *s-simple* if S does not contain any non-void s-ideal different from S. An s-ideal different from S cannot contain any unit in S. The set of non-units forms an s-ideal which therefore will be a uniquely determined maximal s-ideal in S (i. e. no s-ideal is properly lying between $\mathfrak{a}$ and S). From this fact we derive the following characterization of groups in terms of s-ideals:

THEOREM 2. *A commutative semi-group is a group if and only if it is s-simple.*

This characterization is similar to the characterization of a commutative field as a commutative ring R with an identity element which does not contain any d-ideal different from R and the zero ideal. We note, however, in this connection a striking difference between s-ideals and d-ideals. In commutative rings with an identity element one proves the existence of maximal d-ideals by means of Zorn's lemma. (There is, however, an important type of commutative ring with an identity element where the non-units form a d-ideal, namely the socalled *local rings.*) In semi-groups the corresponding fact about s-ideals is independent of Zorn's lemma.

2. Semi-groups with ascending chain condition for s-ideals. We say that the *ascending chain condition* (the descending chain condition is defined in a dual way) for s-ideals holds in the semi-group S, or that S is *s-Noetherian*, if there exists no infinite properly ascending chain of s-ideals

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset \mathfrak{a}_n \subset \ldots$$

where $\mathfrak{a}_i \neq \mathfrak{a}_{i+1}$ for all i. If A is a subset of the semi-group S the intersection of all the s-ideals containing A will be an s-ideal which is said to be generated by A. The s-ideal generated by A is uniquely determined as the least s-ideal containing A. If the s-ideal $\mathfrak{a}$ may be generated by a finite set $A = \{a_1, a_2, \ldots, a_n\}$ we say that $\mathfrak{a}$ is *finitely generated* and write $\mathfrak{a} = (a_1, a_2, \ldots a_n)$. An s-ideal which may be generated by a single element a is called *principal*. Such an ideal (a) consists of all multiples of a. In general the s-ideal generated by A consists of the elements of the product SA.

THEOREM 3. *A commutative semi-group S is s-Noetherian if and only if every s-ideal in S is finitely generated.*

The proof of this theorem is quite similar to the proof of the corresponding well-known theorem on d-ideals and may therefore be omitted. (See for instance [4], p. 169.) We note in passing that this theorem may be generalized considerably. We may for instance prove the following statement: The lattice of all subalgebras of an algebra A satisfies the ascending chain condition if and only if every subalgebra of A is finitely generated. (An even more general formulation of Theorem 3 is found in [3], p. 328, Theorem 2.1.)

The ascending chain condition for s-ideals is much more restrictive than the usual ascending chain condition for d-ideals in ring theory. In order to give an illustration of this let us consider the multiplicative semi-group N consisting of all rational integers. Here for instance

$$(2) \subset (2, 3) \subset (2, 3, 5) \subset \ldots \subset (2, 3, 5, \ldots, p) \subset \ldots$$

constitutes an infinite properly ascending chain of s-ideals where the n'th s-ideal in the chain is generated by the n first prime numbers. (Considering N as a ring, however, every d-ideal is not only finitely generated but even principal.)

3. Determination of the commutative semi-groups satisfying both chain conditions. We shall now determine the semi-groups which satisfy both the ascending and the descending chain condition for s-ideals. To this end we shall first give some definitions and prove a lemma. As remarked in the first section we shall write $a \sim b$ when a and b are associate. The relation $\sim$ is an equivalence relation and if $a \sim b$, $c \sim d$ then $ac \sim bd$. Hence if we denote by $\bar{a}$ the class of elements of S associate to a, we can define the product of two classes $\bar{a}$ and $\bar{b}$ by $\bar{a}\,\bar{b} = \overline{ab}$. The classes of associate elements of S constitute a semi-group $\bar{S}$ homomorphic with S under the mapping $a \to \bar{a}$. $\bar{S}$ has the property that if $\bar{a}$ and $\bar{b}$ are associate in $\bar{S}$ then they are equal. Any semi-group having this property will be called *reduced* and $\bar{S}$ is called the *reduced semi-group* of S. $\bar{S}$ is isomorphic to the semi-group consisting of all principal s-ideals of S, the composition being multiplication.

A family of sets will be called a *ring of sets* when it contains the union and intersection of any two of its sets. We now prove the following

Lemma 1. *If $\mathfrak{R}$ is an infinite ring of sets consisting of subsets of a given set A then $\mathfrak{R}$ contains an infinite chain.*

Proof: We shall prove this lemma by showing that every maximal chain in $\mathfrak{R}$ is necessarily infinite if $\mathfrak{R}$ is infinite. Assuming the axiom of choice $\mathfrak{R}$ certainly contains a maximal chain $\mathfrak{M}$ (cf. [1], pp. 42–44). If $\mathfrak{M}$ were finite we might assume it to have the form

$$M_1 \subset M_2 \subset \ldots \subset M_n\,.$$

If M_1 is different from the void set of A we shall denote this void set by M_0 and if the set M_n is different from A we shall put $M_{n+1} = A$. The sets M_i induce a partition of A in which the difference sets $M_{i+1}-M_i$ $(i = 0, 1, 2, \ldots n)$ form the blocks. Since $\mathfrak{R}$ is infinite $\mathfrak{R}$ will certainly contain a set B which is different from a union of such blocks. There will therefore be a certain block $M_{k+1}-M_k$ which contains both elements belonging to B and elements not belonging to B. This implies that the set $(M_{k+1} \cap B) \cup M_k$ which belongs to $\mathfrak{R}$ can be properly intercalated between M_k and M_{k+1} in contradiction to the fact that $\mathfrak{M}$ is a maximal chain.

THEOREM 4. *A commutative semi-group S satisfies both the ascending and the descending chain conditions for s-ideals if and only if the reduced semi-group of S is finite.*

PROOF: If $\bar{S}$ is finite S will only contain a finite number of principal s-ideals and since every s-ideal is a union of principal s-ideals, $\mathcal{S}$ will also be finite and hence satisfy both chain conditions. Conversely if both chain conditions are satisfied in $\mathcal{S}$ then every chain in $\mathcal{S}$ is finite and since $\mathcal{S}$ is a ring of sets, the above lemma implies that $\mathcal{S}$ must be finite which in turn implies that S contains only a finite number of principal s-ideals; i. e. $\bar{S}$ is finite.

4. s-principal semi-groups. The assumption that all s-ideals in S shall be principal is also much more restrictive than the corresponding assumption about d-ideals in rings. We should, therefore, expect that the semi-groups where all s-ideals are principal have a particularly simple structure. We call such a semi-group *s-principal.* In s-principal semi-groups the ascending chain condition takes the form of the *divisor chain condition*: There exists no infinite sequence of mutually non-associate elements $a_1, a_2, \ldots, a_n, \ldots$ in S such that $a_{i+1}|a_i$ for all i. In an s-principal semi-group the s-ideals are linearly ordered by set inclusion; i. e. the lattice $\mathcal{S}$ is a chain. Otherwise expressed, for any two elements $a, b \in S$ we have either $a|b$ or $b|a$. It is, however, easy to show that the fact that $\mathcal{S}$ is a chain does not imply conversely that S is s-principal. Take for instance, the set S_1 consisting of the real numbers $\geqslant 1$. S_1 forms a semi-group under multiplication and we observe that the s-ideals of S_1 fall into two different classes: On the one hand the closed intervals $[a, \rightarrow[$ consisting of all real numbers $\geqslant a \geqslant 1$ and on the other hand the open intervals $]a, \rightarrow[$ consisting of all real numbers $> a \geqslant 1$. In this case $\mathcal{S}$ is a chain but the s-ideals of the latter kind are neither principal nor even finitely generated. (The s-ideal $]a, \rightarrow[$ may, however, be generated by a *countable* set, namely by a sequence $a_1, a_2, \ldots, a_n, \ldots$ with $a_i > a$ which converges to a.) But if every s-ideal in a semi-group S is finitely generated and $\mathcal{S}$ is a chain then S is s-principal. For let $\mathfrak{a} = (a_1, a_2, \ldots, a_n)$ denote the s-ideal generated by the finite set $\{a_1, a_2, \ldots, a_n\}$. Since $\mathcal{S}$ is a chain, the principal ideals $(a_1), (a_2), \ldots, (a_n)$ will also form a chain. With a suitable enumeration we may assume that

$$(a_1) \subseteq (a_2) \subseteq \ldots \subseteq (a_n)$$

and we get $\mathfrak{a} = (a_n)$, proving that $\mathfrak{a}$ is principal. We may set this down as

Theorem 5. *An s-Noetherian semi-group is s-principal if and only if its lattice of s-ideals is a chain.*

There are further particularities about s-ideals in s-principal semi-groups. We only mention the fact that any s-ideal in such a semi-group will be quasi primary, i. e. have a radical which is prime.

5. Basis representation of s-ideals. If the s-ideal $\mathfrak{a}$ may be generated by the set A but by no proper subset of A we say that A forms a *basis* for $\mathfrak{a}$. A subset A of S is said to be *independent* if for any two different elements $a, b \in A$ we have neither $a|b$ nor $b|a$. We note first the following simple

Lemma 2. *A set A forms a basis for the s-ideal* $\mathfrak{a}$ *if and only if A is an independent set which generates* $\mathfrak{a}$.

Proof: If A generates $\mathfrak{a}$ and is not independent there exist elements $a, b \in A$ such that $a|b$. Then the difference set $A - \{b\}$ still generates $\mathfrak{a}$ and A cannot form a basis for $\mathfrak{a}$. Conversely, if A is independent and generates $\mathfrak{a}$ then no proper subset A' of A can generate $\mathfrak{a}$ since SA' does not contain any element from the difference set $A - A'$ according to the independence of A. Hence A forms a basis for $\mathfrak{a}$.

Theorem 6. *A basis for an s-ideal is uniquely determined apart from associates; i. e. if A and B are bases for the s-ideal* $\mathfrak{a}$ *there exists a one-to-one correspondence between A and B such that if a corresponds to b then a and b are associate. Otherwise expressed: A representation of an s-ideal as an irredundant union of principal s-ideals is unique.*

Proof: If $A = \{a_i\}_{i \in I}$ and $B = \{b_j\}_{j \in J}$ are bases for $\mathfrak{a}$ we have

$$\mathfrak{a} = \bigcup_{i \in I} (a_i) = \bigcup_{j \in J} (b_j).$$

Thus we have in particular for each i

$$(a_i) \subseteq \bigcup_{j \in J} (b_j)$$

which obviously implies that $(a_i) \subseteq (b_j)$ for a certain j. By symmetry $(b_j) \subseteq (a_k)$ for a certain k. Hence $(a_i) \subseteq (a_k)$ or, equivalently, $a_k | a_i$, which implies $a_k = a_i$ according to Lemma 2 since A is independent. This in turn gives $(a_i) = (b_j)$, i. e. the elements a_i and b_j are associate. This evidently proves the theorem.

At first sight one might perhaps expect that every s-ideal has a basis. It would in fact be natural to expect that a maximal independent subset of $\mathfrak{a}$ should form a basis for $\mathfrak{a}$. Such a maximal independent subset exists because the set $\mathfrak{A}$ of independent subsets of $\mathfrak{a}$ forms an inductive set under set-inclusion (i. e. every linearly ordered subset of $\mathfrak{A}$ has an upper bound in $\mathfrak{A}$) so that Zorn's lemma may be applied. As we shall see such a maximal independent subset of $\mathfrak{a}$ need not, however, generate $\mathfrak{a}$. On the other hand one might try to prove the existence of minimal sets in the set $\mathfrak{B}$, constisting of subsets generating $\mathfrak{a}$. Such a minimal subset is, by definition, a basis for $\mathfrak{a}$. But here Zorn's lemma cannot be applied because the set $\mathfrak{B}$ need not be inductive. This stems from the fact that the multiplication is not completely distributive with respect to the operation of intersection, not even if the intersection is only taken over a linearly ordered subset of $\mathfrak{B}$.

We have already considered an example of a semi-group where certain s-ideals do not possess a basis, namely the multiplicative semi-group of all real numbers $\geqslant 1$. A more general example of this kind is found in valuation theory. (Basic information on general valuation theory may be found in § 5 of [6], in [10], and in [5].) Let us consider the multiplicative semi-group S of a valuation ring R defined by a valuation with a non-discrete value group Γ. In such a valuation ring we have for arbitrary elements a, b either $a|b$ or $b|a$ so that the only independent sets that exist are the sets consisting of a single element. Therefore, if every s-ideal in S could be generated by an independent set we should have that every s-ideal in S is principal. This is far from being the case. The elements in S mapped by the given valuation on those elements of Γ which are $> \alpha$ $(\alpha \in \Gamma)$ form an s-ideal in S which cannot be principal, not even finitely generated.

For a given s-ideal $\mathfrak{a}$ there may a priori arise three situations (For general information see [11], in particular 177-179): 1. $\mathfrak{a}$ does not have a basis. 2. $\mathfrak{a}$ has a basis but not every maximal independent subset of $\mathfrak{a}$ is a basis. 3. Every maximal independent subset of $\mathfrak{a}$ forms a basis for $\mathfrak{a}$.

Actually all three situations may arise. Examples of s-ideals of the type 1. have been given above. The examples that may be given of the situation 3. are characterized by the following

THEOREM 7. *A commutative semi-group S is generated by any of its maximal independent subsets if and only if S is a group.*

Proof: The "if"-part of the theorem is obvious. Since $S = (e)$ where e denotes the identity element of S, any basis for S must according to Theorem 6, consist of a single element. Let A be a maximal independent subset containing a given element $a \in S$. Such a maximal independent set exists because the family of independent sets in S which contain the element a is inductive and Zorn's lemma may be applied. According to the condition in the theorem, A is a basis and thus reduces to the single element a. But $(a) = S$, for any $a \in S$ implies that S is a group.

It is also easy to find semi-groups which have s-ideals of type 2. In fact, the s-principal semi-groups which are not groups will be of this kind. For in such a semi-group S there will exist a principal ideal $(a) \neq S$. The element a constitutes a maximal independent subset of S but does not generate S. Valuation rings with a discrete value group form an important example of s-principal semi-groups of this kind. We shall return to valuation rings and valuation semi-groups in a later section. In this section we shall consider instead another example of s-ideals of type 2. Let N_1 be the multiplicative semi-group consisting of all integers $\geqslant 1$. In this semi-group there is a much greater variety of s-ideals than in the semi-group consisting of all real numbers $\geqslant 1$ considered in the foregoing section. It is in fact not quite easy to give a simple and complete classification of all the s-ideals in N_1. We shall here consider only the s-ideals $\mathfrak{a}_n$ consisting of all integers $\geqslant n \geqslant 1$. One verifies easily that $\mathfrak{a}_n$ has a uniquely determined basis consisting of all integers a such that

$$a/p < n \leqslant a \tag{1}$$

for any prime number $p|a$. On the other hand the set of all products of two primes p_1 and p_2 such that $p_1p_2 \geqslant n$ together with the set of all integers a containing at least three prime factors and satisfying (1) for all primes $p|a$ will constitute a maximal independent subset A of $\mathfrak{a}_n$. But A does not form a basis for $\mathfrak{a}_n$ since the primes $\geqslant n$ cannot be generated from A.

6. Irreducible and primary intersection decompositions of s-ideals in s-Noetherian semi-groups. In the paper [14] by Ward and Dilworth a theory of Noether lattices was developed with the purpose of giving a lattice translation of the ideal theory of Noetherian rings. (A *Noether lattice* is a residuated ideal lattice satisfying the ascending chain condition and in which every intersection irreducible element is primary. By a *Noetherian ring* we mean a commutative ring satisfying the ascending chain condition for d-ideals.) In this theory of Ward-Dilworth the basic fact that an irreducible d-ideal is primary had to be postulated since it cannot be proved in the general lattice translation if only the ascending chain condition is assumed. Ward and Dilworth, however, state a theorem ([14], Theorem 11.2) which gives a sufficient condition for a residuated lattice to be a Noether lattice. In [13] this condition is used to show that the lattice $\mathcal{S}$ of all s-ideals of a semi-group S is a Noether lattice if the reduced semi-group $\bar{S}$ is finite. As we have seen (Theorem 4) this means that S satisfies both the ascending and the descending chain condition for s-ideals. The descending chain condition is, however, not necessary for the development of a Noether theory for s-ideals. An important example of a semi-group satisfying the ascending but not the descending chain condition for s-ideals is the multiplicative semi-group of a discrete valuation ring.

Here we shall content ourselves with giving the basic definitions of the Noether theory and a direct proof (making no appeal to the aforementioned theorem in [14]) of the fact that every s-irreducible s-ideal in an s-Noetherian semi-group is primary. Some of the other fundamental results of the Noether theory will only be stated without proofs since in the case of s-ideals these are just the same as in the case of d-ideals.

The s-ideal $\mathfrak{a}$ is said to be *s-irreducible* if $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ implies $\mathfrak{a} = \mathfrak{b}$ or $\mathfrak{a} = \mathfrak{c}$, $\mathfrak{b}$ and $\mathfrak{c}$ being s-ideals. $\mathfrak{p}$ is a *prime* s-ideal if $ab \in \mathfrak{p}$ and $a \notin \mathfrak{p}$ imply $b \in \mathfrak{p}$. The ideal $\mathfrak{q}$ is a *primary* s-ideal if $ab \in \mathfrak{q}$ and $a \notin \mathfrak{q}$ imply $b^n \in \mathfrak{q}$ for some integer n. The *radical* of the s-ideal $\mathfrak{a}$ consists of all elements $s \in S$ such that $s^n \in \mathfrak{a}$ for a certain integer n. The radical of a primary s-ideal $\mathfrak{q}$ is a prime s-ideal which is said to *belong to* $\mathfrak{q}$. By the *quotient* $\mathfrak{a}:\mathfrak{b}$ of two s-ideals $\mathfrak{a}$ and $\mathfrak{b}$ we understand the s-ideal consisting of all elements c satisfying $c\mathfrak{b} \subseteq \mathfrak{a}$. We obviously have

THEOREM 8. *Every s-ideal in an s-Noetherian semi-group may be written as an intersection of a finite number of s-irreducible s-ideals.*

We now prove the basic

THEOREM 9. *In an s-Noetherian semi-group every s-irreducible s-ideal is primary.*

PROOF: Let us assume that the s-ideal $\mathfrak{a}$ is not primary. Then there exist two elements $a, b \in S$ such that $ab \in \mathfrak{a}$, $a \notin \mathfrak{a}$ and $b^n \notin \mathfrak{a}$ for all integers $n \geqslant 1$. The ascending chain condition for s-ideals implies that we must have a certain positive integer k for which

$$\mathfrak{a}:b^k = \mathfrak{a}:b^{k+1}. \tag{2}$$

The reducibility of $\mathfrak{a}$ will now be established by the decomposition

$$\mathfrak{a} = (\mathfrak{a} \cup (a)) \cap (\mathfrak{a} \cup (b^k)). \tag{3}$$

This intersection representation is a proper one since neither a nor b^k belong to $\mathfrak{a}$. We thus have to prove that the right hand side is contained in the left hand side. Using the fact that $\mathcal{S}$ is distributive (Theorem 1) the right hand side of (3) assumes the form

$$(\mathfrak{a} \cap \mathfrak{a}) \cup (\mathfrak{a} \cap (b^k)) \cup (\mathfrak{a} \cap (a)) \cup ((a) \cap (b^k)).$$

Since the first three terms in this union are all contained in $\mathfrak{a}$ we have only to prove that

$$(a) \cap (b^k) \subseteq \mathfrak{a}.$$

Now an element $c \in (a) \cap (b^k)$ belongs to (b^k) and must therefore be of the form sb^k with $s \in S$. Further, since $c = sb^k$ also belongs to (a) we shall have

$$sb^k \in (a) \text{ and } sb^{k+1} \in (ab) \subseteq \mathfrak{a}\ .$$

Finally (2) gives $c = sb^k \in \mathfrak{a}$ which then completes the proof.

From the Theorems 8 and 9 and the fact that the representation of an element of a distributive lattice as an irredundant intersection of irreducible elements is unique (cf. [1], p. 142) we get the following

THEOREM 10. *An s-ideal of an s-Noetherian semi-group may be uniquely represented as an irredundant intersection of a finite number of s-irreducible primary s-ideals.*

In particular we get as a

COROLLARY (Ward-Dilworth [13], p. 604). *By the adjunction of a finite number of elements, every finite commutative semi-group may be embedded in a residuated lattice in which every element, and in particular every element of the original semi-group, may be uniquely represented as an intersection of primary elements.*

Having established that the lattice $\mathcal{S}$ in the case of an s-Noetherian semi-group is a Noether lattice all the well-known decomposition theorems of E. Noether may be derived in the standard way. In particular we have that the intersection of a certain set of primary s-ideals is primary if and only if all the primary s-ideals belong to the same prime s-ideal. Thus contracting the primary s-ideals belonging to the same prime s-ideal we obtain an analogue of the second main decomposition theorem of E. Noether.

THEOREM 11. *Every s-ideal of an s-Noetherian semi-group may be represented as an irredundant intersection of primary s-ideals belonging to mutually different prime s-ideals. The prime s-ideals belonging to the primary s-ideals in such a representation are uniquely determined by the s-ideal represented.*

We shall call such a shortest intersection decomposition of $\mathfrak{a}$ by primary s-ideals an *s-Noether decomposition* of $\mathfrak{a}$. In rings the usual Noether decomposition by d-ideals will be called a *d-Noether decomposition.* The primary s-ideals occurring in an s-Noether decomposition of $\mathfrak{a}$ are called a set of *primary s-components* of $\mathfrak{a}$. The uniquely determined prime s-ideals belonging to a set of primary s-components of $\mathfrak{a}$ are said to *belong to* $\mathfrak{a}$. The prime s-ideals belonging to $\mathfrak{a}$ form a partially ordered set with respect to set inclusion. A primary s-component which belongs to a minimal prime s-ideal of this set is called an *isolated primary s-component* of $\mathfrak{a}$. Just as for d-ideals one may prove

THEOREM 12. *An isolated primary s-component of* $\mathfrak{a}$ *is uniquely determined by the prime s-ideal to which it belongs.*

We note that in contradistinction to the irredundant irreducible decompositions the s-Noether decompositions are not unique. This proves in particular that not all s-Noether decompositions of an s-ideal may in general be obtained from the irreducible decomposition by the contraction process.

7. Application to rings.

Let R be a commutative ring with an identity element and let S be its multiplicative semi-group (i. e. S is composed of the same elements as R and organized by a single operation, called multiplication, which is the multiplication of R). In the rest of the paper the prefix s always refers to the s-concepts in S while the prefix d refers to the ordinary (Dedekindian) ideal concept in R. The use of the prefix x shall mean that the sentence in which it occurs is valid both for $x = d$ and $x = s$.

The lattice of all d-ideals in R is always modular but in general not distributive. On the other hand a theorem of Dilworth [2] says that every element of a lattice L admits of a unique irredundant representation as an intersection of irreducibles if and only if L is a semi-modular lattice in which every modular sublattice is distributive. Combining these two facts it follows from pure lattice-theory that the irredundant decomposition of a d-ideal as an intersection of d-irreducible d-ideals is not always unique. Since the corresponding decomposition by means of s-ideals is unique, it follows that the irredundant decomposition of a d-ideal into an intersection of d-irreducible d-ideals will in general contain fewer terms than the irredundant decomposition of the same d-ideal into an intersection of s-irreducible s-ideals. Otherwise expressed a d-irreducible d-ideal may be s-reducible. In an s-Noetherian ring we therefore have that two irredundant d-irreducible decompositions of a d-ideal always possess a common refinement by the introduction of s-ideals. Thus if R is s-Noetherian we may in general attach two different integers to a given d-ideal: I_d = the number of terms in an irredundant intersection representation by d-irreducible d-ideals and I_s = the number of terms in an irredundant intersection representation by s-irreducible s-ideals. $I_d \leqslant I_s$ and in general $I_d < I_s$. It is of some interest to note that the situation is different as concerns the Noether decompositions. If we denote the number of terms in a d-Noether decomposition of a given d-ideal by N_d and the number of terms in an s-Noether decomposition of the same d-ideal by N_s, we have $N_d = N_s$. For it is clear that any d-Noether decomposition of a d-ideal $\mathfrak{a}$ in R is also an s-Noether decomposition of $\mathfrak{a}$. This gives

Theorem 13. *The prime s-ideals belonging to a given d-ideal in a d-Noetherian ring are all d-ideals. Further an isolated primary s-component is also a d-ideal.*

In particular the minimal prime s-ideals containing a given d-ideal in a d-Noetherian ring is itself a d-ideal. More generally any minimal prime set (i. e. a subset A of R with the property that $ab \in A$, $a \in A$ imply $b \in A$) containing the x-ideal $\mathfrak{a}$ in a d-Noetherian ring will be an x-ideal. Similar remarks also apply to minimal 'half prime sets' in their relation to half prime x-ideals ($\mathfrak{a}$ is half-prime if $\mathfrak{a}$ is identical with its radical).

We shall now give a simple illustration of a ring R where we actually have $I_d < I_s$. According to the above-mentioned theorem of Dilworth concerning the unicity of irreducible decompositions we should seek an s-Noetherian ring which has a non-unique irredundant intersection decomposition of d-ideals into d-irreducible d-ideals among those rings whose lattice of d-ideals is non-distributive. To find for instance a finite ring with this property is simple. The simplest non-distributive but modular lattice is the one represented by the following lattice diagram

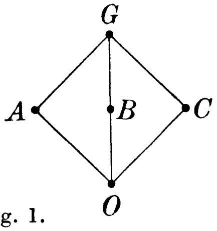

Fig. 1.

and this lattice is isomorphic with the lattice of all subgroups of the (commutative) *four-group*. We shall denote this additive group by $G = \{o, a, b, c\}$; o being the zero element of G. The proper subgroups are $A = \{o, a\}$, $B = \{o, b\}$, $C = \{o, c\}$ and $O = \{o\}$. We therefore have only to define a multiplication over G in such a way that we get a commutative ring R in which all the additive subgroups are d-ideals in R. This can be done only in the trivial way by putting $ab = 0$ for all $a, b \in G$. In this ring R we have three distinct irredundant decompositions of the zero ideal as an intersection of d-irreducible d-ideals

$$O = A \cap B = A \cap C = B \cap C\,. \tag{4}$$

In R a subset T is an s-ideal if and only if T contains the zero element of R. In addition to the d-ideals we therefore have that the following subsets of R form s-ideals: $D = \{0, a, b\}$, $E = \{0, a, c\}$ and $F = \{0, b, c\}$. The lattice of all s-ideals in R therefore takes the form

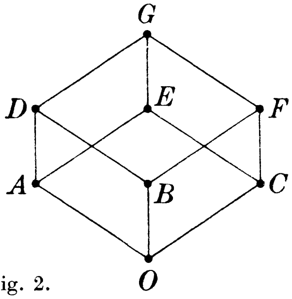

Fig. 2.

which is a Boolean algebra isomorphic with the lattice of all subsets of a set with three elements. The unique irreducible decomposition of O in this lattice will be

$$O = D \cap E \cap F$$

which just represents the common refinement of the three decompositions (4). In this example $I_d = 2$, $I_s = 3$ and $N_d = N_s = 1$ since O is primary. It is however not clear from this example that in an s-Noether decomposition of a d-ideal there may really occur terms that are not d-ideals.

8. Remarks on valuation theory. Integral domains where every s-ideal is a *d*-ideal. In the foregoing we referred on various occasions to examples from valuation theory. In the present section we shall give some general remarks on valuations of groups in connection with the problem of characterizing the rings where every s-ideal is a d-ideal.

The classical examples of an exponential valuation in ring theory are those associated with the prime ideals of a Dedekindian domain I, i. e. an integral domain, where every proper d-ideal admits a unique factorization into a finite product of prime d-ideals. In the valuation $v_{\mathfrak{p}}$ (defined by the prime ideal $\mathfrak{p} \subseteq I$) the value attached to the element

$a = bc^{-1}$ lying in the quotient field K of I $(b, c \in I)$ is the difference between the exponents of $\mathfrak{p}$ in the unique prime ideal decompositions of the principal ideals (b) and (c). These valuations have the three well-known properties: 1° v is a univalued mapping of the non zero elements of K onto the additive group Z of rational integers. 2° $v(ab) = v(a)+v(b)$. 3° $v(a+b) \geqslant \min\big(v(a), v(b)\big)$. These three properties are then taken to be the defining properties of a general (exponential) valuation of a field K when the value group Z is replaced by an arbitrary linearly ordered group Γ. If P is a partially ordered set with respect to an order relation $\leqslant$ (i.e. if it satisfies the conditions $\alpha \leqslant \alpha$, $\alpha \leqslant \beta \;\&\; \beta \leqslant \gamma \rightarrow \alpha \leqslant \gamma$, and $\alpha \leqslant \beta \;\&\; \beta \leqslant \alpha \rightarrow \alpha = \beta$) we say that P is a *partially ordered abelian group* if P is at the same time an abelian group (under an operation denoted additively) and satisfies the homogeneity condition $\alpha \leqslant \beta \rightarrow \alpha+\gamma \leqslant \beta+\gamma$ for every $\gamma \in P$. P is *linearly ordered* if for any $\alpha, \beta \in P$ either $\alpha \leqslant \beta$ or $\beta \leqslant \alpha$ holds good.

The most important example of an exponential valuation in the theory of groups and semi-groups is afforded by the following consideration (which is slightly more general than the situation arising from prime ideals in Dedekindian domains). Let S be a regular commutative semi-group which may be embedded in a Gaussian semi-group T; i.e. S is isomorphic with a subsemi-group S' of a semi-group T admitting an essentially unique factorization of its elements into products of multiplicatively irreducible elements. (For a precise definition of a Gaussian semi-group see [4], p. 115.) If $a \in S$ corresponds to $a' \in S'$ by this isomorphism we shall write $a \longleftrightarrow a'$. With respect to an irreducible element $p_i \in T$ we may now define a valuation v_{p_i} of the quotient group G of S (defined in the usual way by means of formal quotients ab^{-1}, $a \in S$, $b \in S$) onto the additive group Z of rational integers. The value of $a \in S$ is defined as the exponent belonging to the irreducible element p_i in the unique decomposition of a' within T. Thus, if

$$a \longleftrightarrow a' = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$$

is the decomposition of a' into irreducibles, we define $v_{p_i}(a) = \alpha_i$. Now an element $a = bc^{-1} = b/c$ in G corresponds to an element b'/c' in the quotient group G' of S' by the isomorphism which extends the isomorphism between S and S'. The element b'/c' may be written uniquely as

$$\frac{b'}{c'} = \frac{p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n}}{p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_n^{\gamma_n}}$$

where $p_1, p_2, \ldots, p_n$ may be taken to be the irreducible factors of the product $b'c'$. Here $\beta_i \geqslant 0$, $\gamma_i \geqslant 0$ and we put $p_i^0 = e'$ (the identity element of S'). We may therefore write each element of G' symbolically as a unique product

$$a \longleftrightarrow a' = b'/c' = p_1^{\beta_1-\gamma_1}p_2^{\beta_2-\gamma_2}\dots p_n^{\beta_n-\gamma_n} = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_n^{\alpha_n}$$

and define $v_{p_i}(a) = \alpha_i$. Evidently v_{p_i} is a univalued mapping of G onto Z which satisfies $v_{p_i}(ab) = v_{p_i}(a)+v_{p_i}(b)$.

We now define a *valuation* of an abelian group G as a univalued homomorphic mapping of G onto a linearly ordered group Γ. Denoting the operation in G multiplicatively and the operation in Γ additively this means that the mapping v defines a valuation of G if: 1° The range of v is a linearly ordered group Γ. 2° $v(ab) = v(a)+v(b)$. The valuation v is said to be *non-trivial* if Γ consists of at least two elements. According to a well-known theorem an abelian group G may be linearly ordered if and only if every element different from the identity element e of G has an infinite order. Thus an abelian group G admits a non-trivial valuation if and only if G has a homomorphic image consisting of at least two elements and in which every element $\neq e$ has an infinite order. In particular the finite groups do not possess non-trivial valuations.

If P is a partially ordered set we call a subset A of P an *upper class* if $\alpha \in A$ implies $\beta \in A$ whenever $\beta \geqslant \alpha$. The upper class A is said to be *generated* by the set $\{\alpha_i\}_{i\in I}$ if A consists of all elements β such that $\beta \geqslant \alpha_i$ for at least one α_i and we shall write $A = P\{\alpha_i\}$. If the set $\{\alpha_i\}_{i\in I} = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ is finite we shall write $A = P\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ and say that A is *finitely generated.* An element $\alpha \geqslant 0$ is said to be *non-negative.* The *valuation semi-group* S of G with respect to the valuation v of G is the set of all elements in G mapped on non-negative elements of Γ by v. In analogy with the situation in ring theory there is a one-to-one correspondence between the s-ideals of S and the upper classes of non-negative elements of Γ. More generally there is a one-to-one correspondence between the fractional ideals of S and the upper classes of P. If the s-ideal $\mathfrak{a}$ corresponds to the upper class A, a set of generators for $\mathfrak{a}$ is mapped by v on a set of generators for A, and conversely any set of elements of $\mathfrak{a}$ which has a set of generators of A as its range will form a set of generators for $\mathfrak{a}$. Since every upper class in Γ either may be generated by a single element or is not finitely generated, it follows that an s-ideal in a valuation semi-group S is either principal or cannot be finitely generated. If Γ is discrete in its order topology every s-ideal in S is principal. In the case that Γ is non-discrete the principal s-ideals correspond to the closed upper classes (i. e. the upper classes possessing a least element) in Γ while non-finitely generated s-ideals correspond to the open upper classes in Γ.

We have already remarked that in a valuation ring all s-ideals are d-ideals. (If K is a field over which a valuation v is defined the *valuation ring* in K with respect to v is the set consisting of the zero element of K and all elements of K mapped upon non-negative elements of Γ by v.) We shall now show that, conversely, if I is an integral domain in which every s-ideal is a d-ideal then I is a valuation ring. In fact this will be an immediate consequence of the following slightly more general

THEOREM 14. *A necessary and sufficient condition that every s-ideal of a commutative ring R with an identity element be a d-ideal is that for any two elements $a, b \in R$ either $a|b$ or $b|a$ holds.*

PROOF: If neither $a|b$ nor $b|a$ the set-theoretical union of the two principal ideals (a) and (b) forms an s-ideal which is not a d-ideal since $(a) \cup (b)$ cannot contain the element $a+b$. Conversely, let a and b be two elements of an s-ideal $\mathfrak{a}$ of R. If for instance we suppose that $a|b$, i. e. $b = ac$ $(c \in R)$, we get $a-b = a-ac = a(e-c) \in \mathfrak{a}$ and $\mathfrak{a}$ is a d-ideal.

It is a fundamental fact in the general valuation theory that an integral domain I is a valuation ring if and only if for any two elements $a, b \in I$ either $a|b$ or $b|a$ holds (cf. for instance [5], p. 165, Satz 1). We thus get the following

COROLLARY. *An integral domain I is a ring where all s-ideals are d-ideals if and only if I is a valuation ring.*

REFERENCES

1. G. Birkhoff, *Lattice theory*, Revised edition, New York, 1948.
2. R. P. Dilworth, *Lattices with unique irreducible decompositions*, Ann. of Math. 41 (1940), 771–777.
3. G. Higman, *Ordering by divisibility in abstract algebras*, Proc. London Math. Soc. (3) 2 (1952), 326–336.
4. N. Jacobson, *Lectures in abstract algebra* 1, New York, 1951.
5. W. Krull, *Allgemeine Bewertungstheorie*, J. reine angew. Math. 167 (1932), 160–196.
6. W. Krull, *Idealtheorie* (Ergebnisse d. Mathematik u. ihrer Grenzgebiete 4.3), Berlin, 1935.
7. P. Lorenzen, *Abstrakte Begründung der multiplikativen Idealtheorie*, Math. Z. 45 (1939), 533–553.
8. P. Lorenzen, *Über halbgeordnete Gruppen*, Math. Z. 52 (1949), 483–526.
9. H. Prüfer, *Untersuchungen über Teilbarkeitseigenschaften in Körpern*, J. reine angew. Math. 168 (1932), 1–36.
10. O. F. G. Schilling, *The theory of valuations* (Mathematical Surveys 4), New York 1950.
11. J. Schmidt, *Über die Rolle der transfiniten Schlussweisen in einer allgemeinen Idealtheorie*, Math. Nachr. 7 (1952), 165–182.
12. M. Ward, *Residuated distributive lattices*, Duke Math. J. 6 (1940), 641–651.
13. M. Ward and R. P. Dilworth, *The lattice theory of ova*, Ann. of Math. 40 (1939), 600–608.
14. M. Ward and R. P. Dilworth, *Residuated lattices*, Trans. Amer. Math. Soc. 45 (1939), 335–354.

UNIVERSITY OF OSLO, NORWAY, P.T. PARIS, FRANCE