NOTE ON THE KUROSCH-ORE THEOREM

R. P. DILWORTH

1. Introduction. The Kurosch-Ore theorem[1] asserts that if an element of a modular lattice has two decompositions into irreducibles, then each irreducible of one decomposition may be replaced by a suitably chosen irreducible from the other decomposition. It follows that the number of irreducibles in the two decompositions is the same.

The purpose of the present note is to study the manner in which the irreducibles of two decompositions can replace one another. Now from the Kurosch-Ore theorem it is not even clear that each irreducible of one decomposition is suitable for replacing some irreducible of the other decomposition. However, this follows from the following precise theorem:

THEOREM 1. *Let a be an element of a modular lattice and let $a=q_1\cap\cdots\cap q_n=q_1'\cap\cdots\cap q_n'$ be two reduced decompositions into irreducibles. Then the q's may be renumbered in such a way that*

$$a = q_1\cap\cdots\cap q_{i-1}\cap q_i'\cap q_{i+1}\cap\cdots\cap q_n, \qquad i = 1, \cdots, n.$$

Along the same line of ideas, the following theorem on simultaneous replacement is also proved.

THEOREM 2. *Let a be an element of a modular lattice and let $a=q_1\cap\cdots\cap q_n=q_1'\cap\cdots\cap q_n'$ be two reduced decompositions into irreducibles. Then for each q_i, there exists q_j' such that q_j' can replace q_i in the first decomposition and q_i can replace q_j' in the second decomposition.*

On the other hand, an example is given which shows that, in general, it is impossible to renumber the q's in such a way that simultaneously q_i may replace q_i' and q_i' replace q_i.

As the principal tool in the investigation we introduce the concept of a *superdivisor* r of an element a. r has the fundamental property that its crosscut with any proper divisor of a is never equal to a. The superdivisors of a are closed under crosscut and indeed form a dual-ideal $\mathfrak{r}_a$ which properly divides a.

A surprising by-product of the investigation is the fact that in a

Presented to the Society, September 8, 1942, under the title *On the decomposition theory of modular lattices*; received by the editors April 9, 1946.

[1] A simple proof is given in Birkhoff [1, p. 54]. Numbers in brackets refer to the references cited at the end of the paper.

modular lattice satisfying the ascending chain condition, $\mathfrak{r}_a$ can be used to prove the existence of covering ideals. Thus, in this case, the customary use of transfinite induction can be avoided.

2. Properties of superdivisors. Let M denote a modular lattice of elements $a, b, c, \cdots$. $a \supseteq b$ will denote ordinary lattice inclusion while $a \supset b$ will denote proper inclusion. We recall that an element q of M is (crosscut) irreducible if $q = x \cap y$ implies either $q = x$ or $q = y$.

DEFINITION 1. A divisor r of a is a *superdivisor* of a if $r \cap x = a$ implies $x = a$ for all x in M.

The following lemmas give the basic properties of superdivisors.[2]

LEMMA 1. *If r is a superdivisor of a and $s \supseteq r$, then s is a superdivisor of a.*

For $s \cap x = a$ implies $r \cap x = a$ implies $x = a$.

LEMMA 2. *If r and s are superdivisors of a, then $r \cap s$ is a superdivisor of a.*

For $(r \cap s) \cap x = a$ implies $r \cap (s \cap x) = a$ implies $s \cap x = a$ implies $x = a$.

COROLLARY. *The superdivisors of a form a dual-ideal $\mathfrak{r}_a$ of M.*

LEMMA 3. *If q is an irreducible divisor of a and $x \supset q$, then x is a superdivisor of a.*

For if $x \cap y = a$, then $q = q \cup a = q \cup (x \cap y) = x \cap (q \cup y)$ by the modular law. Since q is irreducible and $q \neq x$, it follows that $q = q \cup y$. Hence $y = q \cap y = q \cap x \cap y = q \cap a = a$. Thus x is a superdivisor of a.

Now if $a = q_1 \cap \cdots \cap q_n$ is a reduced decomposition of a into irreducibles, we shall set $Q_i = q_1 \cap \cdots \cap q_{i-1} \cap q_{i+1} \cap \cdots \cap q_n$. Clearly $a = q_i \cap Q_i$ and $Q_i \neq a$.

LEMMA 4. *Let $a = q_1 \cap \cdots \cap q_n$ be a reduced decomposition into irreducibles. Then if r is a superdivisor of a, $q_i \cup (r \cap Q_i)$ is also a superdivisor of a.*

By Lemma 3 if $q_i \cup (r \cap Q_i)$ is not a superdivisor of a, then $q_i \supseteq r \cap Q_i$. But then $r \cap Q_i = r \cap q_i \cap Q_i = a$. Hence $Q_i = a$ which contradicts $Q_i \neq a$.

LEMMA 5. *Let $a = q_1 \cap \cdots \cap q_n$ be a reduced decomposition into ir-*

[2] If the descending chain condition holds, it is easy to show that r is a superdivisor if and only if $r \supseteq u_a$ where u_a is the union of the elements covering a. Cf. Dilworth [2, p. 288].

reducibles and let $x \supseteq r_1 \cap Q_1, r_2 \cap Q_2, \cdots, r_i \cap Q_i$ *where* $r_1, \cdots, r_i$ *are superdivisors of* a. *Then* $x \supseteq r \cap q_{i+1} \cap \cdots \cap q_n$ *where* r *is a superdivisor of* a.

Now clearly $x \supseteq r \cap q_1 \cap \cdots \cap q_n$ for any superdivisor r of a. Let k be maximal such that $x \supseteq r \cap q_k \cap \cdots \cap q_n$ for some superdivisor r. Suppose $k \leqq i$. Then by the hypothesis of the lemma $x \supseteq r_k \cap Q_k$. Let $r' = r \cap r_k$. Then $x \supseteq (r' \cap q_k \cap \cdots \cap q_n) \cup (r' \cap Q_k) = r' \cap q_{k+1} \cap \cdots \cap q_n \cap (q_k \cup (r' \cap Q_k))$. But $q_k \cup (r' \cap Q_k)$ is a superdivisor of a by Lemma 4. Hence $r' \cap (q_k \cup (r' \cap Q_k)) = r''$ is a superdivisor of a by Lemma 2. But then $x \supseteq r'' \cap q_{k+1} \cap \cdots \cap q_n$ contrary to the maximal property of k. Thus $k > i$ and the conclusion of the lemma follows.

3. **Decomposition theory.** The application of superdivisors to decomposition problems rests on the following lemma:

LEMMA 6. *Let* $a = q_1 \cap \cdots \cap q_n$ *be a reduced decomposition of* a. *Then* q_i *may be replaced by an irreducible divisor* q *of* a *if and only if* $q \supseteq r \cap Q_i$ *is false for every superdivisor* r *of* a.

Let us suppose that q can replace q_i. Then $a = q \cap Q_i$. Hence if $q \supseteq r \cap Q_i$ for some superdivisor r, then $r \cap Q_i = r \cap q \cap Q_i = r \cap a = a$ and $Q_i = a$ which is impossible. Thus $q \supseteq r \cap Q_i$ fails for every superdivisor r. Conversely suppose $q \supseteq r \cap Q_i$ holds for no superdivisors r. Then

$$q \supseteq q \cap Q_i = (q \cap Q_i) \cup (q_i \cap Q_i) = [q_i \cup (q \cap Q_i)] \cap Q_i.$$

Hence $q_i \cup (q \cap Q_i)$ is not a superdivisor of a and by Lemma 3 we have $q_i \supseteq q \cap Q_i$. Thus $q \cap Q_i = q \cap q_i \cap Q_i = a$ and q can replace q_i in the decomposition.

The theorems stated in the introduction can now be proved.

PROOF OF THEOREM 1. Let S_i' denote the set of irreducibles of the second decomposition which can replace q_i in the first decomposition. Now suppose that there are k of the sets S_i' which together contain less than k irreducibles. Renumbering if necessary, we can suppose that $S_1', \cdots, S_k'$ are composed of the irreducibles $q_1', \cdots, q_l'$ where $l < k$. It follows that q_j' cannot replace q_i if $j > l$ and $i \leqq k$. Hence by Lemma 6, $q_j' \supseteq r_{ji} \cap Q_i$ for some superdivisor r_{ji} of a if $j > l$ and $i \leqq k$. From Lemma 5 we conclude that $q_j' \supseteq r_j \cap q_{k+1} \cap \cdots \cap q_n$ for some superdivisor r_j of a if $j > l$. Thus $q_{l+1}' \cap \cdots \cap q_n' \supseteq r \cap q_{k+1} \cap \cdots \cap q_n$ where $r = r_{l+1} \cap \cdots \cap r_n$ is a superdivisor of a. But then

$$a = q_1' \cap \cdots \cap q_l' \cap q_{l+1}' \cap \cdots \cap q_n' \supseteq r \cap q_1' \cap \cdots \cap q_l' \cap q_{k+1} \cap \cdots \cap q_n \supseteq a.$$

Hence $a = r \cap q_1' \cap \cdots \cap q_l' \cap q_{k+1} \cap \cdots \cap q_n$. Since r is a superdivisor of a, we have

$$a = q_1' \cap \cdots \cap q_l' \cap q_{k+1} \cap \cdots \cap q_n.$$

Since $l<k$, the number of components in this decomposition is less than n, contrary to the Kurosch-Ore theorem. Thus every k of the sets S_i' contain at least k irreducibles. It follows from the Radó-Hall theorem on representatives of sets that there exists a distinct set of representatives for the sets $S_1', \cdots, S_n'$. Renumbering if necessary, we may suppose that these representatives are $q_1', \cdots, q_n'$. But then q_i' can replace q_i and the theorem is proved.

Proof of Theorem 2. Renumbering if necessary, we may suppose that $q_1', \cdots, q_l'$ can replace q_i while the others cannot. According to Lemma 6, $q_j' \supseteq r_j \cap Q_i$, $j=l+1, \cdots, n$, where r_j is s superdivisor of a. Now suppose that q_i can replace none of the irreducibles $q_1', \cdots, q_l'$ in the second decomposition. Again by Lemma 6 we have $q_i \supseteq r_j' \cap Q_j'$, $j=1, \cdots, l$. From Lemma 5 we conclude that $q_i \supseteq r' \cap q_{l+1}' \cap \cdots \cap q_n'$ for some superdivisor r'. Now $q_{l+1}' \cap \cdots \cap q_n' \supseteq r_{l+1} \cap \cdots \cap r_n \cap Q_i = r \cap Q_i$ where r is a superdivisor of a. Hence $q_i \supseteq r' \cap r \cap Q_i$ where $r' \cap r$ is a superdivisor of a. But then $r' \cap r \cap Q_i = r' \cap r \cap Q_i \cap q_i = a$ and $Q_i = a$ contrary to hypothesis. Hence q_j' can be replaced by q_i for some $j \leqq l$. Thus q_i and q_j' can replace one another.

In order to see that a sharper theorem on simultaneous replacement cannot be proved in general, consider the lattice of subspaces of the seven-point projective plane. If $1, \cdots, 7$ denote the points, let the lines (and the points they contain) be denoted by $l_1(124)$, $l_2(235)$, $l_3(346)$, $l_4(457)$, $l_5(156)$, $l_6(267)$, $l_7(137)$. $l_1, \cdots, l_7$ are the irreducibles of the lattice. Let us consider the decompositions of the null space z. We have

$$z = l_1 \cap l_2 \cap l_3 = l_5 \cap l_6 \cap l_7.$$

Now the possible sets of replacements of l_1, l_2, l_3 respectively are (l_5, l_6, l_7), (l_6, l_5, l_7), and (l_6, l_7, l_5). But l_1, l_2, l_3 is a possible set of replacements only for (l_5, l_7, l_6), (l_7, l_5, l_6), and (l_7, l_6, l_5). Hence it is not possible in this case to renumber the irreducibles in such a way that corresponding irreducibles can replace one another.

4. Existence of covering ideals. It is well known that the lattice of dual-ideals of a lattice M contains M as the sublattice of principal ideals.[3] Hence if $\mathfrak{a}$ is a dual-ideal, by $\mathfrak{a} \supseteq a$ we shall mean $\mathfrak{a} \supseteq (a)$ where

[3] For the general properties of dual-ideals used in this paper see Dilworth [3, pp. 329–331].

(a) is the principal ideal generated by a. Also $\mathfrak{a} > a$ ($\mathfrak{a}$ "covers" a) means $\mathfrak{a} \supset a$ and no ideal exists which properly contains $\mathfrak{a}$ and is properly contained in (a). We give a proof of the existence of covering ideals which does not require transfinite induction.

THEOREM 3. *Let an element a of a modular lattice M have a decomposition into irreducibles. Then if $\mathfrak{a} \supseteq a$, there exists a dual-ideal $\mathfrak{p}$ such that $\mathfrak{a} \supseteq \mathfrak{p} > a$.*

PROOF. Let $\mathfrak{a}' = \mathfrak{a} \cap \mathfrak{r}_a$ where $\mathfrak{r}_a$ is the dual-ideal of all superdivisors of a. Then $\mathfrak{a}' \neq (a)$. For if $\mathfrak{a}' = (a)$, then $x \cap r = a$ where $x \in \mathfrak{a}$ and r is a superdivisor of a. But then $x = a$ and $\mathfrak{a} = (a)$ contrary to $\mathfrak{a} \supset a$. Now let $a = q_1 \cap \cdots \cap q_n$ be a reduced decomposition of a into irreducibles. Clearly $\mathfrak{r}_a \cap q_1 \cap \cdots \cap q_{i-1} \supseteq \mathfrak{r}_a \cap q_1 \cap \cdots \cap q_i$. Suppose $\mathfrak{r}_a \cap q_1 \cap \cdots \cap q_{i-1} = \mathfrak{r}_a \cap q_1 \cap \cdots \cap q_i$. Then $\mathfrak{r}_a \cap q_1 \cap \cdots \cap q_{i-1} \cap q_{i+1} \cap \cdots \cap q_n = a$ and hence $r \cap Q_i = a$ where r is a superdivisor of a. Thus $Q_i = a$ contrary to assumption. Next suppose that $\mathfrak{r}_a \cap q_1 \cap \cdots \cap q_{i-1} \supset \mathfrak{b} \supset \mathfrak{r}_a \cap q_1 \cap \cdots \cap q_i$. Then since the lattice of dual-ideals is modular we have $\mathfrak{b} = \mathfrak{r}_a \cap q_1 \cap \cdots \cap q_{i-1} \cap (\mathfrak{b} \cup q_i)$. Let $b \in \mathfrak{b}$. If $q_i \supseteq b$, then $q_i \supseteq \mathfrak{b}$ and $\mathfrak{b} = \mathfrak{r}_a \cap q_1 \cap \cdots \cap q_{i-1} \cap q_i$ contrary to hypothesis. Hence $q_i \cup b$ is a proper divisor of q_i for every $b \in \mathfrak{b}$. By Lemma 3, $q_i \cup b$ is a superdivisor of a for every $b \in \mathfrak{b}$. Hence $q_i \cup b \in \mathfrak{r}_a$ for every $b \in \mathfrak{b}$. Thus $q_i \cup \mathfrak{b} \supseteq r_a$. But then $\mathfrak{b} = \mathfrak{r}_a \cap q_1 \cap \cdots \cap q_{i-1}$ contrary to assumption. Thus $\mathfrak{r}_a \cap q_1 \cap \cdots \cap q_{i-1} > \mathfrak{r}_a \cap q_1 \cap \cdots \cap q_i$. But then $\mathfrak{r}_a > \mathfrak{r}_a \cap q_1 > \cdots > \mathfrak{r}_a \cap q_1 \cap \cdots \cap q_{n-1} > a$ is a finite complete chain joining $\mathfrak{r}_a$ to a. By the general theory of modular lattices (Birkhoff [1]) it follows that the quotient lattice $\mathfrak{r}_a/a$ is of finite dimension. Since $\mathfrak{a}' \in \mathfrak{r}_a/a$ we have $\mathfrak{a}' \supseteq \mathfrak{p} > a$ for some dual-ideal $\mathfrak{p}$ and the theorem is proved.

Now if the ascending chain condition holds in a modular lattice M, then every element has a decomposition into irreducibles and hence, by Theorem 3, there exist dual-ideals covering a for every a not the unit of M.

REFERENCES

1. G. Birkhoff, *Lattice theory*, Amer. Math. Soc. Colloquium Publications, vol. 25, 1940.

2. R. P. Dilworth, *Arithmetical theory of Birkhoff lattices*, Duke Math. J. vol. 8 (1941) pp. 286–299.

3. ———, *Ideals in Birkhoff lattices*, Trans. Amer. Math. Soc. vol. 49 (1941) pp. 325–353.

CALIFORNIA INSTITUTE OF TECHNOLOGY