RING HOMOMORPHISMS WHICH ARE ALSO LATTICE HOMOMORPHISMS.*

By Morgan Ward.

1. Given two homomorphic rings $\mathfrak{O}$ and $\mathfrak{O}'$: what lattice properties of the rings are preserved under the homomorphism; more specifically, if $\mathfrak{O}$ is a lattice, will $\mathfrak{O}'$ be a homomorphic lattice? [1] It is easily seen that if $\mathfrak{S}$ and $\mathfrak{S}'$ are the lattices of ideals of $\mathfrak{O}$ and $\mathfrak{O}'$, any ring homomorphism of $\mathfrak{O}$ to $\mathfrak{O}'$ induces a lattice homomorphism of $\mathfrak{S}$ to $\mathfrak{S}'$. Unfortunately, when $\mathfrak{O}$ is a lattice with respect to the usual division relation, it need not be a sublattice of $\mathfrak{S}$. The homomorphism $\mathfrak{S}$ to $\mathfrak{S}'$ consequently gives little information about the lattice properties of $\mathfrak{O}'$.

If we assume however that the ascending chain condition holds in the lattice $\mathfrak{O}$, it is not difficult to show that $\mathfrak{O}$ is a sublattice of $\mathfrak{S}$ if and only if every ideal of $\mathfrak{O}$ is principal and $\mathfrak{O}$ and $\mathfrak{S}$ are lattice isomorphic. The object of this paper is to show in this case that all homomorphic rings $\mathfrak{O}'$ are also lattices of a very simple structure.

For the case when $\mathfrak{O}$ is a domain of integrity, my results may be more easily obtained from the fact that the fundamental theorem of arithmetic holds in every "principal ideal ring." (van der Waerden 1). The interest of the present investigation is that $\mathfrak{O}$ is merely required to be a commutative ring with a unit element. The methods used are based upon a theory of residuated lattices which have been developed by Mr. R. P. Dilworth and myself in a series of recent papers.[2]

2. Let $\mathfrak{O}$ be a commutative ring with a unit element, all of whose ideals are principal.

Definition 2.1. Division in $\mathfrak{O}$. *If a and b are any two elements of $\mathfrak{O}$, a is said to divide b if and only if the principal ideal (a) contains the principal ideal (b). If (a) equals (b), a and b are said to be equivalent.*

We write $a \supset b$, $a \sim b$. $\mathfrak{O}$ evidently forms a semi-ordered set with respect

* Received December 16, 1938.

[1] This problem was propounded to me by Professor E. T. Bell for the special case when $\mathfrak{O}$ is the ring of rational integers.

[2] Ward, 1, 2; Ward-Dilworth, 1, 2.

to the relation $x \supseteq y$, and $x \sim y$ is an equivalence relation. Furthermore $a \supset b$ if and only if there exists an element c such that $ac = b$.

THEOREM 2.1. *The ascending chain condition holds for the elements of* $\mathfrak{O}$.

That is, if we have a chain of elements $a_1, a_2, a_3, \cdots$ such that $a_1 \subset a_2 \subset a_3 \subset \cdots$, then from a certain point on, all elements are equivalent to one another. It obviously suffices to show that in the ascending chain of ideals $(a_1) \subset (a_2) \subset (a_3) \subset \cdots$ all ideals are equal from a certain point on. The proof may be carried out exactly as in van der Waerden 1, § 17.

THEOREM 2.2. *The ideals of* $\mathfrak{O}$ *form a distributive residuated lattice.*

Proof. The ideals of any ring form a modular lattive $\mathfrak{S}$ over which a multiplication may be defined with the properties given in Ward 1. Since the ascending chain condition holds for ideals by the previous theorem, a residual may also be introduced, so that the lattice is residuated by definition. (Ward-Dilworth 1.) Since all ideals $\mathfrak{a}$, $\mathfrak{b}$ of $\mathfrak{O}$ are principal, $\mathfrak{a}$ contains $\mathfrak{b}$ if and only if there exists an ideal $\mathfrak{i}$ such that $\mathfrak{a}\mathfrak{i} = \mathfrak{b}$. Hence the lattice is distributive. (Ward-Dilworth 2, theorem 16.2).

3. We next consider the lattice formed by the elements of $\mathfrak{O}$.

THEOREM 3.1. *If a and b are any two elements of* $\mathfrak{O}$, *there exists an element d with the properties*

(i) $d \supset a$, $d \supset b$.
(ii) $x \supset a$, $x \supset b$ *imply* $x \supset d$.
(iii) $d = ua + vb$ *for some* u, v *of* $\mathfrak{O}$,
(iv) d *is determined up to equivalence.*

Proof. Consider the ideal $((a), (b)) = (a, b)$. Since all ideals are principal, $(a, b) = (d)$. Hence (i) follows and (iii) follows. Then (ii) follows from (iii), and (iv) from (ii).

We write $a \sim (a, b)$, and call d a union of a and b.

THEOREM 3.2. *If a and b are any two elements of* $\mathfrak{O}$, *there exists an element m such that*

(i) $a \supset m$, $b \supset m$.
(ii) $a \supset y$, $b \supset y$ *imply* $m \supset y$.
(iii) m *is determined up to equivalence.*

Proof. Consider the ideal $[(a), (b)]$. Since it is principal, $[(a), (b)] =$

(m). The element m is easily seen to have the required properties. We write $m \sim [a, b]$, and call m a cross-cut of a and b.

It follows from theorem 3.1 and 3.2 that $\mathfrak{O}$ forms a lattice with respect to the division relation $x \supset y$.

THEOREM 3.3. *$\mathfrak{O}$ forms a residuated lattice with respect to division relation $x \supset y$ and the multiplication operation xy of $\mathfrak{O}$.*

Proof. We need only show that the multiplication has the properties given in Ward 1, p. 629, for then by theorem 3.2, a residual may be introduced (Ward 1) so that $\mathfrak{O}$ will be residuated by definition. All of these properties are evident save the rule $a(b, c) \sim (ab, ac)$. Now $(b, c) = bu + cw$ by theorem 3.1 (iii) for some u, w of $\mathfrak{O}$. Hence $a(b, c) = abu + acw$. Therefore $(ab, ac) \supset a(b, c)$. But since $(b, c) \supset b$ and c, $a(b, c) \supset ab$, ac. Hence by theorem 3.1 (ii), $a(b, c) \supset (ab, ac)$. Therefore $(ab, ac) \sim a(b, c)$.

THEOREM 3.4. *$\mathfrak{O}$ is a distributive lattice.*

Proof. The correspondence $a \rightarrow (a)$ is a lattice isomorphism, since "equal elements" (that is equivalent elements in $\mathfrak{O}$) correspond to equal elements in $\mathfrak{S}$ and vice versa. Since $\mathfrak{S}$ is distributive by theorem 2.3, $\mathfrak{O}$ is distributive.

THEOREM 3.5. *Every element of $\mathfrak{O}$ may be uniquely represented up to equivalence as a cross-cut of primary elements none of which divides any other.*

Proof. With the terminology of Ward-Dilworth 2, $\mathfrak{O}$ is a distributive residuated lattice in which every element is principal. The result thus follows from theorem 14.2 of Ward-Dilworth 2, theorem 8.4 of Ward 2 and the remarks in section 12 of Ward-Dilworth 2.

4. Consider any homomorphism of the ring $\mathfrak{O}$. The homomorphism is completely specified by an ideal $\mathfrak{m}$, and its residue classes. Since $\mathfrak{m}$ is a principal ideal (m), $a \equiv b \pmod{\mathfrak{m}}$ if and only if $a = b + qm$ for some element q of $\mathfrak{O}$. Denote the residue classes of congruent elements modulo $\mathfrak{m}$ by $A, B, \cdots$. We wish to make these classes into a lattice. We begin by extending definition 2.1.

DEFINITION 4.1. DIVISION MODULO $\mathfrak{m}$. *An element a of $\mathfrak{O}$ is said to divide another element b of $\mathfrak{O}$ modulo $\mathfrak{m}$ if and only if there exists an element c such that $ac \equiv b$ (mod $\mathfrak{m}$).*

We write $a \supset b$ (*mod* $\mathfrak{m}$).

DEFINITION 4.2. EQUIVALENCE MODULO $\mathfrak{m}$. *Two elements a and b of $\mathfrak{O}$ are said to be equivalent modulo $\mathfrak{m}$ if and only if each divides the other modulo $\mathfrak{m}$.*

We write $a \sim b \pmod{\mathfrak{m}}$.

$\mathfrak{O}$ forms a semi-ordered set with respect to the relation of division modulo $\mathfrak{m}$, and equivalence modulo $\mathfrak{m}$ is an equivalence relation in the technical sense. It is evident furthermore that we have

THEOREM 4.1. *$a \supset b$ modulo $\mathfrak{m}$ if and only if there exist elements r and s such that $b = ar + ms$.*

We may note also that $a \sim b$ or $a \equiv b$ mod $\mathfrak{m}$ imply $a \sim b \pmod{\mathfrak{m}}$, and $a \supset b$ implies $a \supset b \pmod{\mathfrak{m}}$. Hence the relations of division and equivalence modulo $\mathfrak{m}$ may be immediately extended to the residue classes $A, B, \cdots$ of $\mathfrak{O}$ modulo $\mathfrak{m}$.

THEOREM 4.2. *If $\mathfrak{m} = (m)$, then* (i) *$a \supseteq b \pmod{\mathfrak{m}}$ if and only if $(a, m) \supset b$ in $\mathfrak{O}$, and* (ii) *$a \sim b \pmod{\mathfrak{m}}$ if and only if $(a, m) \sim (b, m)$.*

Proof. (i) By theorem 3.1 (iii), $(a, m) \sim al + km$, l, m elements of $\mathfrak{O}$. Hence $(a, m) \supset b$ implies that $b = (al + km)q = aql + mqk$. Therefore by theorem 4.1, $(a, m) \supset b$ implies that $a \supset b \pmod{\mathfrak{m}}$. Next, if $a \supset b \pmod{\mathfrak{m}}$, then by theorem 4.1, $b = ar + ms$. Hence by theorem 3.1 (i), $(a, m) \supset b$.

(ii) If both $a \supset b \pmod{\mathfrak{m}}$ and $b \supset a \pmod{\mathfrak{m}}$, then $(a, m) \supset b$ and $(b, m) \supset a$. Hence $(a, m) \supset (b, m)$ and $(b, m) \supset (a, m)$ or $(a, m) \sim (b, m)$. The converse is evident.

THEOREM 4.3. $a \sim (a, m) \pmod{\mathfrak{m}}$.

Proof. $(a, m) \sim ((a, m), m)$.

THEOREM 4.4. *The correspondence $x \to x^* \sim (x, m)$ is a lattice homomorphism of $\mathfrak{O}$.*

Proof. Assume that $a \to a^*$ and $b \to b^*$. Then

$$(a, b)^* \sim (a, b), m) \sim ((a, m), (b, m)) \sim (a^*, b^*).$$

Since $\mathfrak{O}$ is a distributive lattice we also have

$$[a, b]^* \sim ([a, b], m) \sim [(a, m), (b, m)] \sim [a^*, b^*],$$

We observe that the correspondence of theorem 4.4 maps the lattice $\mathfrak{O}$ onto the sublattice of divisors of m in $\mathfrak{O}$.

THEOREM 4.5. *If $a \rightarrow a^*$ and $b \sim a$ (mod $\mathfrak{m}$), then $b^* \sim a^*$, and conversely.*

Proof. $a \rightarrow a^*$ if and only if $a^* \sim (a, m)$ and $a \sim b$ (mod $\mathfrak{m}$) if and only if $(a, m) \sim (b, m)$.

THEOREM 4.6. *The residue classes $A, B, \cdots$ of $\mathfrak{O}$ modulo $\mathfrak{m}$ form a lattice with respect to the relation of division modulo $\mathfrak{m}$ which is isomorphic with the lattice of the divisors of $\mathfrak{m}$ in $\mathfrak{O}$ if equivalent classes modulo $\mathfrak{m}$ and equivalent divisors are not regarded as distinct.*

Proof. We assign to A the element $a^* \sim (a, m)$, a any element of A. (We may if we please make the correspondence entirely definite by replacing a^* by the ideal $\mathfrak{a} = ((a), (m)) = (a^*))$. Then since $a \equiv b$ (mod $\mathfrak{m}$) implies $a \sim b$ (mod $\mathfrak{m}$), a^* is, up to equivalence, independent of the particular element of A used in defining it. By theorem 4.5, $A \sim B$ (mod $\mathfrak{m}$) if and only if $a^* \sim b^*$ and by theorem 4.2, $A \supset B$ (mod $\mathfrak{m}$) if and only if $a^* \supset b^*$. The result then follows from theorem 4.4.

PASADENA, CALIFORNIA.

REFERENCES

Morgan Ward, 1. *Duke Mathematical Journal*, vol. 3 (1937), pp. 627-636; 2. *Annals of Mathematics*, vol. 39 (1938), pp. 558-568.

Morgan Ward-R. P. Dilworth, 1. *Proceedings of the National Academy of Sciences*, vol. 24 (1938), pp. 162-164; 2. *Transactions of the American Mathematical Society.*

van der Waerden, 1. *Moderne Algebra*, vol. 1 (Berlin, 1930).