NON-COMMUTATIVE ARITHMETIC

BY R. P. DILWORTH

1. Introduction and summary. The problem of determining the conditions that must be imposed upon a system having a single associative and commutative operation in order to obtain unique factorization into irreducibles has been studied by A. H. Clifford [1],[1] König [1], and Ward [2]. The more general problem of determining similar conditions for the non-commutative case has been treated by M. Ward [1]. However, the conditions given by Ward are more stringent than those satisfied by actual instances of non-commutative arithmetic, for example, quotient lattices and non-commutative polynomial theory (Ore [1, 2]). Moreover, in both of these instances the factorization is unique only up to a similarity relation, and instead of a single operation of multiplication the additional operations G. C. D. and L. C. M. are involved.[2] Accordingly, we shall concern ourselves with the arithmetic of a non-commutative multiplication defined over a lattice.

As the decomposition of lattice quotients gives an important instance of non-commutative arithmetic, we shall summarize here a few of the fundamental ideas of Ore's theory (Ore [1]). Let Σ be the set of quotients[3]

$$\alpha = \frac{a_1}{a_2}, \qquad a_2 \supset a_1, \qquad a_1, a_2 \epsilon L,$$

where L is a lattice in which the ascending chain condition holds. If $\beta = b_1/b_2$, we define $(\alpha, \beta) = (a_1, b_1)/(a_2, b_2)$, $[\alpha, \beta] = [a_1, b_1]/[a_2, b_2]$. With these definitions Σ is a lattice which is modular or distributive if and only if L is modular or distributive. Ore defines the product $\alpha \cdot \beta$ only for elements $\alpha, \beta \epsilon \Sigma$ such that $a_2 = b_1$, in which case $\alpha \cdot \beta = a_1/b_2$. Let us set $\alpha \simeq \beta$ if and only if $a_2 = b_1$, so that a necessary and sufficient condition for the existence of the product $\alpha \cdot \beta$ is that $\alpha \simeq \beta$. Although the relation $\simeq$ is neither reflexive nor symmetric, it is in a certain sense transitive since

$$\text{(1)} \qquad \text{if } \alpha \simeq \beta \text{ and } \gamma \simeq \delta, \text{ then } \gamma \simeq \beta \text{ implies } \alpha \simeq \delta.$$

Furthermore, the relation is preserved under union and cross-cut; that is,

$$\text{(2)} \qquad \alpha \simeq \beta,\ \gamma \simeq \delta \text{ implies } (\alpha, \gamma) \simeq (\beta, \delta),\ [\alpha, \gamma] \simeq [\beta, \delta].$$

Received September 2, 1938.

[1] The numbers in brackets refer to the references at the end of the paper.

[2] In this regard note that the necessary and sufficient conditions for unique factorization in the commutative case are stated in their most elegant form in terms of the G. C. D. operation (König [1]).

[3] Our inclusion is the reverse of Ore's.