AN APPLICATION OF LATTICE THEORY TO QUASIGROUPS

M. F. SMILEY

The purpose of this note is to show that O. Ore's general formulation of the Jordan-Hölder theorems in partially ordered sets[1] [3] yields the Jordan-Hölder theorems for loops [1] which have recently been obtained by A. A. Albert [2]. We shall assume that the reader is familiar with the papers [1, 2, 3] of O. Ore and of A. A. Albert.

We begin with an examination of certain congruence relations in loops. We are led to characterize the normal divisors of A. A. Albert as those subloops which commute and associate with the elements of the loop. Our proof of the fundamental quadrilateral condition of O. Ore [3] is then based on this characterization.

A *loop* $\mathfrak{G}$ is a quasigroup with an identity element e. For each non-null subset $\mathfrak{H} \subset \mathfrak{G}$ we define a relation H_ρ on $\mathfrak{G}\mathfrak{G}$ as follows:

(1) *If* $x, y \in \mathfrak{G}$, *then* $xH_\rho y$ *in case* $y \in x\mathfrak{H}$.

THEOREM 1. *The relation* H_ρ *is a congruence relation for the loop* $\mathfrak{G}$ *if and only if*

$$\text{(i) } x \in (xh)\mathfrak{H}, \qquad \text{(ii) } (x\mathfrak{H})(y\mathfrak{H}) \subset (xy)\mathfrak{H}$$

for every $x, y \in \mathfrak{G}$ *and* $h \in \mathfrak{H}$.

PROOF. Let H_ρ be a congruence relation for $\mathfrak{G}$. For each $x \in \mathfrak{G}$ and $h \in \mathfrak{H}$ we have $xH_\rho(xh)$ by the definition of H_ρ. Since H_ρ is symmetric we have $(xh)H_\rho x$, $x \in (xh)\mathfrak{H}$. If also $y \in \mathfrak{G}$, $h_1 \in \mathfrak{H}$, then $yH_\rho(hy_1)$, and since H_ρ preserves multiplication we obtain $(xy)H_\rho(xh)(hy_1)$, $(xh)(yh_1) \in (xy)\mathfrak{H}$. Conversely, let $\mathfrak{H}$ satisfy (i) and (ii). If $x \in \mathfrak{G}$, choose $h \in \mathfrak{H}$ and we have $x \in (xh)\mathfrak{H} \subset x\mathfrak{H}$ by (i) and (ii). Thus H_ρ is reflexive. If also $y \in \mathfrak{G}$ and $xH_\rho y$, we have $y = xh_1$, and (i) yields $x \in (xh_1)\mathfrak{H} = y\mathfrak{H}$, $yH_\rho x$. Thus H_ρ is symmetric. If also $z \in \mathfrak{G}$ and $yH_\rho z$, we have $z = yh_2 = (xh_1)h_2 \in x\mathfrak{H}$ by (ii). Thus H_ρ is transitive and is an equivalence relation. The relations $xH_\rho y$, $zH_\rho w$ yield $(xz)H_\rho(yw)$ by (ii) and we conclude that H_ρ is a congruence relation for $\mathfrak{G}$.

Remark 1. If R is a congruence relation for a loop $\mathfrak{G}$, then the subset $\mathfrak{R} \equiv [x; xRe]$ is a *subloop* of $\mathfrak{G}$. For clearly $e \in \mathfrak{R}$ and $\mathfrak{R}$ is closed with

Presented to the Society, April 29, 1944; received by the editors April 8, 1944. The opinions and assertions contained in this paper are the private ones of the author and are not to be construed as official or reflecting the views of the United States Navy Department or of the naval service at large.

[1] Numbers enclosed in brackets denote the references given at the end of the paper.

respect to multiplication. If we have $r_1x=r_2$, then eRr_1, xRx give $xR(r_1x)$, xRr_2, r_2Re, xRe, $x\in\mathfrak{R}$. Similarly $xr_1=r_2$ implies $x\in\mathfrak{R}$ and $\mathfrak{R}$ is a subloop of $\mathfrak{G}$. With $R=H_\rho$, we obtain $\mathfrak{R}=\mathfrak{H}$ and thus (i) and (ii) imply that $\mathfrak{H}$ is a subloop of $\mathfrak{G}$. (For groups $\mathfrak{G}$, every congruence relation R is of the form H_ρ for suitable $\mathfrak{H}\subset\mathfrak{G}$.)

Remark 2. We note the following consequences of (i) and (ii):

$$x(y\mathfrak{H}) \subset (xy)\mathfrak{H}, \tag{2}$$

$$(x\mathfrak{H})y \subset (xy)\mathfrak{H}, \tag{3}$$

$$x(\mathfrak{H}y) \subset (xy)\mathfrak{H}, \tag{4}$$

$$\mathfrak{H}x \subset x\mathfrak{H}. \tag{5}$$

For *finite* $\mathfrak{H}$ each of these inequalities[2] is an *equality*. To see this for (2), note that for fixed x, $y\in\mathfrak{G}$ we have a single-valued mapping $h\to h^*$ defined by $x(yh)=(xy)h^*$. This mapping is one-to-one since $x(yh_1)=x(yh_2)$ implies $h_1=h_2$. For a finite $\mathfrak{H}$, we conclude that the set of images $[h^*]=\mathfrak{H}$, and consequently that $(xy)\mathfrak{H}=x(y\mathfrak{H})$. The same reasoning applies to the inequalities (3), (4), and (5). It is now easy to see that if $\mathfrak{H}$ is a *finite* subloop of $\mathfrak{G}$, then H_ρ is a congruence relation for $\mathfrak{G}$ if and only if the set $\mathfrak{H}$ commutes and associates with the elements of $\mathfrak{G}$ in the sense that

$$x\mathfrak{H} = \mathfrak{H}x, \tag{6}$$

$$(xy)\mathfrak{H} = x(y\mathfrak{H}), \qquad (x\mathfrak{H})y = x(\mathfrak{H}y), \qquad (\mathfrak{H}x)y = \mathfrak{H}(xy) \tag{7}$$

for every x, $y\in\mathfrak{G}$.

THEOREM 2. *A subloop $\mathfrak{H}$ of a loop $\mathfrak{G}$ satisfies* (6) *and* (7) *if and only if $\mathfrak{H}$ is a normal divisor of $\mathfrak{G}$ in the sense of A. A. Albert.*

PROOF. Consider a subloop $\mathfrak{H}$ of a loop $\mathfrak{G}$ which satisfies (6) and (7). The permutation group $\mathfrak{H}_\rho$ generated by the right multiplication of $\mathfrak{G}$ gives rise to the cosets $x\mathfrak{H}_\rho$ of Albert. We first show that the cosets $x\mathfrak{H}_\rho=x\mathfrak{H}$. Clearly $x\mathfrak{H}_\rho\supset x\mathfrak{H}$. The elements of $\mathfrak{H}_\rho$ are finite products of permutations of the form R_h and R_h^{-1} for $h\in\mathfrak{H}$. If $y=xR_h^{-1}$, then $yh=x$, $y=y(hh_1)=(yh)h_2=xh_2$, $y=xR_{h_2}$. It follows that each element of $x\mathfrak{H}_\rho$ may be written in the form $xh\in x\mathfrak{H}$. We next note that

$$(x\mathfrak{H})(y\mathfrak{H}) = (xy)\mathfrak{H} \tag{8}$$

is an immediate consequence of (6) and (7). To see that the cosets $x\mathfrak{H}$ form a loop we now consider the equations

[2] This result is due to G. N. Garrison. See §4 of his fundamental paper, *Quasigroups*, Ann. of Math. vol. 41 (1940) pp. 474–487.

$$(9) \qquad (x\mathfrak{H})(w\mathfrak{H}) = y\mathfrak{H}, \qquad (z\mathfrak{H})(x\mathfrak{H}) = y\mathfrak{H}.$$

Solutions of (9) are provided by the solutions of $xw=y$ and $zx=y$ for w and z. The uniqueness of the solutions $w\mathfrak{H}$ and $z\mathfrak{H}$ of (9) is readily verified. We have proved that $\mathfrak{G}/\mathfrak{H}$ is a loop and hence that $\mathfrak{H}$ is a normal divisor of $\mathfrak{G}$ in the sense of A. A. Albert.

To prove the converse it suffices to use the representation $\mathfrak{H}=e\Gamma$ furnished by Albert's Theorem 3 [1]. Using this theorem, the verifications of (6) and (7) are quite simple and we shall omit them.

Remark 3. The equations (6) and (7) may be replaced by

$$(10) \qquad (x\mathfrak{H})y = x(y\mathfrak{H}),$$

$$(11) \qquad (xy)\mathfrak{H} = x(y\mathfrak{H})$$

for every $x, y\in\mathfrak{G}$. To see this, set $x=e$ in (10) to obtain (6).

THEOREM 3. *The intersection $\mathfrak{H}$ of a system $(\mathfrak{H}_\alpha;\ \alpha\in\Omega)$ of normal divisors of a loop $\mathfrak{G}$ is a normal divisor of $\mathfrak{G}$.*

PROOF. Clearly $\mathfrak{H}$ is a subloop of $\mathfrak{G}$. We shall prove $\mathfrak{H}x\subset x\mathfrak{H}$ for every $x\in\mathfrak{G}$. If $h\in\mathfrak{H}$, $\alpha\in\Omega$, we have $hx=xh_\alpha$ for some $h_\alpha\in\mathfrak{H}_\alpha$. The left cancellation law then shows that the set $[h_\alpha;\ \alpha\in\Omega]$ is singular and its sole member is an element of $\mathfrak{H}$. The remainder of the proof consists in a repetition of this argument which proves (6) and (7).

COROLLARY. *The set of all normal divisors of a loop $\mathfrak{G}$, when ordered by set inclusion, forms a complete lattice.*

PROOF. It suffices to remark that $\mathfrak{G}$ is a normal divisor of $\mathfrak{G}$. We shall use $\cup$ and $\cap$ to denote the lattice operations of this lattice.

THEOREM 4. *If $\mathfrak{H}$ and $\mathfrak{K}$ are normal divisors of a loop $\mathfrak{G}$, then $\mathfrak{H}\mathfrak{K}$ is a normal divisor of $\mathfrak{G}$ and $\mathfrak{H}\mathfrak{K}=\mathfrak{H}\cup\mathfrak{K}$.*

PROOF. Clearly $e\in\mathfrak{H}\mathfrak{K}$ and $\mathfrak{H}\mathfrak{K}$ is closed with respect to multiplication. Now if $x(hk)=h_1k_1$, we use (7) to get $(xh)k_2=h_1k_1$. Two applications of (i) and use of (6) and (7) then give $x=h_3k_3$. We compute $x(\mathfrak{H}\mathfrak{K})=(x\mathfrak{H})\mathfrak{K}=(\mathfrak{H}x)\mathfrak{K}=\mathfrak{H}(x\mathfrak{K})=\mathfrak{H}(\mathfrak{K}x)=(\mathfrak{H}\mathfrak{K})x$. Thus $\mathfrak{H}\mathfrak{K}$ is a subloop of $\mathfrak{G}$ satisfying (6). We omit the simple verification of (7). Since every normal divisor of $\mathfrak{G}$ which contains $\mathfrak{H}$ and $\mathfrak{K}$ must contain $\mathfrak{H}\mathfrak{K}$, we conclude that $\mathfrak{H}\mathfrak{K}=\mathfrak{H}\cup\mathfrak{K}$.

COROLLARY. *The lattice of normal divisors of a loop $\mathfrak{G}$ is modular.*

THEOREM 5 (QUADRILATERAL CONDITION). *If $\mathfrak{H}$ and $\mathfrak{K}$ are maximal normal divisors of a loop $\mathfrak{G}$, then $\mathfrak{H}\cap\mathfrak{K}$ is a maximal normal divisor of the loop $\mathfrak{H}$, and $\mathfrak{G}/\mathfrak{K}\cong\mathfrak{H}/\mathfrak{H}\cap\mathfrak{K}$.*

PROOF. Suppose on the contrary that $\mathfrak{L}$ is a normal divisor of the loop $\mathfrak{H}$ such that $\mathfrak{H} \succ \mathfrak{L} \succ \mathfrak{H} \cap \mathfrak{K}$. We shall prove that $\mathfrak{L}\mathfrak{K}$ is a normal divisor of $\mathfrak{G}$. We note that $\mathfrak{G} = \mathfrak{H}\mathfrak{K}$ and to verify (10) we consider the equation

$$[(hk)(h_1k_1)](h_2k_2) = (hk)[(h_2k_2)(h_3k_3)]$$

which we may write, using (8), (i), and (7) for $\mathfrak{K}$, as

$$(hh_1)h_2 = [h(h_2h_3)]k_4. \tag{12}$$

Now if $h_1 \in \mathfrak{L}$, we may use (10) for $\mathfrak{L}$ to get $h(h_2l) = [h(h_2h_3)]k_4$. We now use (7) for $\mathfrak{K}$, cancel h, use (7) for $\mathfrak{K}$ again and cancel h_2 to obtain $l = h_3k_5$. It follows that $k_5 \in \mathfrak{H}$, and hence that $k_5 \in \mathfrak{H} \cap \mathfrak{K} \subset \mathfrak{L}$. Consequently $h_3 \in \mathfrak{L}$ and we have proved $[x(\mathfrak{L}\mathfrak{K})]y \subset x[y(\mathfrak{L}\mathfrak{K})]$ for every x, $y \in \mathfrak{G}$. On the other hand, if $h_3 \in \mathfrak{L}$, we may use (10) for $\mathfrak{L}$ to get $(hh_1)h_2 = [(hl)h_2]k_4$. We now use (6) and (7) for $\mathfrak{K}$ and cancel h_2, use (6) and (7) for $\mathfrak{K}$ and cancel h to obtain $h_1 = lk_5$ from which $h_1 \in \mathfrak{L}$ follows as before. This completes the verification of (10). We apply the same reasoning to verify (11). We write

$$[(hk)(h_1k_1)](h_2k_2) = (hk)[(h_1k_1)(h_3k_3)]$$

as $(hh_1)h_2 = [h(h_1h_3)]k_4$. Then if $h_2 \in \mathfrak{L}$, we have $h(h_1l) = h[(h_1h_3)k_5]$ and we easily obtain $h_3 \in \mathfrak{L}$. Also, if $h_3 \in \mathfrak{L}$, we have $(hh_1)h_2 = (hh_1)(lk_5)$, $h_2 = lk_5$, $h_2 \in \mathfrak{L}$. Thus (11) holds for $\mathfrak{L}\mathfrak{K}$. To show that $\mathfrak{L}\mathfrak{K}$ is a subloop of $\mathfrak{G}$ it now suffices to note that $e \in \mathfrak{L}\mathfrak{K}$, $(\mathfrak{L}\mathfrak{K})(\mathfrak{L}\mathfrak{K}) = \mathfrak{L}\mathfrak{K}$, and to prove that if $(hk)(l_1k_1) = l_2k_2$, then $h \in \mathfrak{L}$. But we may write this equation as $hl_1 = l_2k_4$ and get $h = h(l_1l_3) = (hl_1)l_4 = l_5k_5$. As before, $k_5 \in \mathfrak{L}$, $h \in \mathfrak{L}$. We have proved that $\mathfrak{L}\mathfrak{K}$ is a normal divisor of $\mathfrak{G}$. Note also that $\mathfrak{G} \succ \mathfrak{L}\mathfrak{K} \succ \mathfrak{K}$, since if $h \in \mathfrak{H}$ and h does not belong to $\mathfrak{L}$, then $hk = lk_1$ implies $h = lk_2$, $k_2 \in \mathfrak{L}$, $h \in \mathfrak{L}$, a contradiction, and $\mathfrak{L} \succ \mathfrak{H} \cap \mathfrak{K}$. Our assumption of the existence of a normal divisor $\mathfrak{L}$ of $\mathfrak{H}$ satisfying $\mathfrak{H} \succ \mathfrak{L} \succ \mathfrak{H} \cap \mathfrak{K}$ has led to a contradiction of the assumption that $\mathfrak{K}$ is a maximal normal divisor of $\mathfrak{G}$. We conclude that $\mathfrak{H} \cap \mathfrak{K}$ is a maximal normal divisor of $\mathfrak{H}$.

To establish the isomorphism we map the cosets $x\mathfrak{K}$ of $\mathfrak{G}/\mathfrak{K}$ onto the cosets $x(\mathfrak{H} \cap \mathfrak{K})$ of $\mathfrak{H}/\mathfrak{H} \cap \mathfrak{K}$. This mapping exhausts the set $\mathfrak{H}/\mathfrak{H} \cap \mathfrak{K}$ and is one-to-one. For, if $x(\mathfrak{H} \cap \mathfrak{K}) = y(\mathfrak{H} \cap \mathfrak{K})$, then $xk = yu$ gives $x = (yu)k_1 = yk_2$, $uk_3 = k_2$, $u \in \mathfrak{K}$, $x\mathfrak{K} \subset y\mathfrak{K}$, and symmetry yields $x\mathfrak{K} = y\mathfrak{K}$. That this mapping preserves multiplication in the two loops $\mathfrak{G}/\mathfrak{H}$ and $\mathfrak{H}/\mathfrak{H} \cap \mathfrak{K}$ is evident. The proof is complete.

Theorem 5 is the main tool which is needed to apply Ore's result [3] to the partially ordered set of subloops of a loop $\mathfrak{G}$ which occur in some composition series of $\mathfrak{G}$.

REFERENCES

1. A. A. Albert, *Quasigroups.* I, Trans. Amer. Math. Soc. vol. 54 (1943) pp. 507–519.
2. ———, *Quasigroups.* II, Trans. Amer. Math. Soc. vol. 55 (1944) pp. 401–419.
3. O. Ore, *Chains in partially ordered sets,* Bull. Amer. Math. Soc. vol. 49 (1943) pp. 558–566.

UNITED STATES NAVAL ACADEMY, POSTGRADUATE SCHOOL

TWO ELEMENT GENERATION OF A SEPARABLE ALGEBRA

A. A. ALBERT

The *minimum rank* of an algebra A over a field F is defined to be the least number $r=r(A)$ of elements $x_1, \cdots, x_r$ such that A is the set of all polynomials in $x_1, \cdots, x_r$ with coefficients in F. In what follows we shall assume that A is an *associative algebra of finite order* over an *infinite* field F.

It is well known that $r(A)=1$ if A is a separable field over F and that $r(A)=2$ if A is a total matric[1] algebra over F. Over fourteen years ago I obtained but did not publish the result that $r(A)=2$ if A is a central division algebra over F. The purpose of this note is to provide a brief proof of the generalization which states that if A is any *separable* algebra over F then $r(A)=1$ or 2 according as A is or is not commutative.

We observe first that a commutative separable[2] algebra Z is a direct sum of separable fields and that there exists a scalar extension K over F such that Z_K has a basis $e_1, \cdots, e_n$ over F for pairwise orthogonal idempotents e_i. If $u_1, \cdots, u_n$ is a basis of Z over F and $x=a_1u_1+\cdots+a_nu_n$ the powers x^i have the form

$$x^i = \sum_{j=1}^{n} b_{ij}u_j \qquad (i = 1, \cdots, n),$$

where the determinant

$$d(a_1, \cdots, a_n) = |b_{ij}|$$

is a polynomial in the parameters $a_1, \cdots, a_n$. If $c_1, \cdots, c_n$ are any

Received by the editors April 13, 1944.

[1] See page 95 of my *Modern higher algebra.*

[2] The definition of a separable algebra given below reduces to a direct sum of fields in the commutative case. When F is nonmodular the concept of semisimple algebra and separable algebra coincide.