QUASIGROUPS. I

BY

A. A. ALBERT

1. **Introduction.** A theory of non-associative algebras has been developed[1] without any assumption of a substitute for the associative law, and the basic structure properties of such algebras have been shown to depend upon the possession of almost these same properties by related associative algebras.

It seems natural then to attempt to obtain an analogous treatment of quasigroups. We shall present the results here. Most of the results in the literature on quasigroups do depend upon special associativity conditions[2] but no assumption of such conditions is necessary for our theorems.

Every quasigroup $\mathfrak{G}$ may be associated with the group $\mathfrak{G}_\tau$ of nonsingular transformations generated by its multiplications. The isotopy of two quasigroups may then be defined and, as in the case of algebras, two groups (that is associative quasigroups) are isotopic if and only if they are isomorphic. Every quasigroup is isotopic to a *loop*, that is, a quasigroup with an identity element, and we derive all further results for loops.

The concepts of *coset* and *normal divisor* may be defined for loops without any assumption of associativity[3]. Then a subloop $\mathfrak{H}$ of $\mathfrak{G}$ is a normal divisor of $\mathfrak{G}$ if and only if $\mathfrak{H} = e\Gamma$ where e is the identity of $\mathfrak{G}$ and Γ is a normal divisor of the group $\mathfrak{G}_\tau$. Isotopic loops have corresponding normal divisors, and loops which are isotopic to simple loops are simple. We also combine the con-

_____

Presented to the Society, September 13, 1943. Received by the editors June 17, 1943.

[1] See the paper of N. Jacobson, *A note on non-associative algebras*, Duke Math. J. vol. 3 (1937) pp. 544–548, as well as the author's papers *Non-associative algebras. I. Fundamental concepts and isotopy*, Ann. of Math. vol. 43 (1942) pp. 686–707; *The radical of a non-associative algebra*, Bull. Amer. Math. Soc. vol. 48 (1942) pp. 891–897.

[2] Cf. A. Suschkewitsch, *On a generalization of the associative law*, Trans. Amer. Math. Soc. vol. 31 (1929) pp. 204–214. A suggestion of isotopy theory is given there and the assumption is made that the right multiplications form a group. Then he shows that the quasigroup is isotopic to a group. See also D. C. Murdoch, *Quasigroups which satisfy certain generalized associative laws*, Amer. J. Math. vol. 61 (1939) pp. 509–522; ibid., *Structure of abelian quasigroups*, Trans. Amer. Math. Soc. vol. 49 (1941) pp. 392–409; H. Griffin, *The abelian quasigroups*, Amer. J. Math. vol. 62 (1940) pp. 725–737.

[3] In this connection see B. A. Hausman and O. Ore, *Theory of quasigroups*, Amer. J. Math. vol. 59 (1937) pp. 983–1004. These authors determined associativity conditions in order that the classical coset decompositions be valid. A similar idea was used by D. C. Murdoch, *Note on normality in quasigroups*, Bull. Amer. Math. Soc. vol. 47 (1941) pp. 134–138 but not by G. N. Garrison, in his *Quasigroups*, Ann. of Math. vol. 41 (1940) pp. 474–487, who also discussed the concept of normal divisor but used the finiteness of the system in an essential way. The definition we shall give here for loops seems to be much more natural than these others and reduces to the classical definition in the case of groups.

cepts of isotopy and homorphism to yield a new concept of *homotopy*[4] of loops. Then we show that if a loop $\mathfrak{G}$ is homotopic to a loop $\mathfrak{G}'$ it is homomorphic to a loop which is isotopic to $\mathfrak{G}'$.

2. Permutation groups. A *transformation* on a set $\mathfrak{G}$ is defined to be a correspondence

$$S: \qquad\qquad g \to gS$$

on $\mathfrak{G}$ to $\mathfrak{G}$. If the correspondence is one-to-one it is usually called a nonsingular correspondence. It will be convenient here to refer to nonsingular transformations as *permutations*. This is standard usage in the case where $\mathfrak{G}$ is a finite set and there seems to be no reason why the terminology should not be extended to the general case.

The set Σ of *all* permutations of $\mathfrak{G}$ forms a group with respect to the operation of product defined by $g(ST) = (gS)T$. It is customary to call this group the *symmetric* group.

If Γ is any set of permutations of $\mathfrak{G}$, and g is any element of $\mathfrak{G}$, we define $g\Gamma$ to be the set of all elements gS for S in Γ. When Γ is a subgroup of Σ it contains the identity transformation I and $g\Gamma$ contains $gI = g$.

We call a subset $\mathfrak{H}$ of $\mathfrak{G}$ a *transitive system* for a permutation group Γ on $\mathfrak{G}$ if hS is in $\mathfrak{H}$ for every h of $\mathfrak{H}$ and S of Γ and if, for every h and k of $\mathfrak{H}$, there is an S in Γ such that $k = hS$. Then we have the following simple lemma:

LEMMA 1. *The transitive systems $\mathfrak{H}$ for a permutation group Γ on $\mathfrak{G}$ are the sets $\mathfrak{H} = h_0\Gamma$ for h_0 any element of $\mathfrak{H}$.*

For if $\mathfrak{H} = h_0\Gamma$ then every element of $\mathfrak{H}$ has the form $h = h_0S$, $(h_0S)T = h_0(ST)$ is in $\mathfrak{H}$. Also $h = h_0S$, $k = h_0T$ implies that $k = (h_0S^{-1})T = h_0(S^{-1}T)$ for $S^{-1}T$ in Γ. Conversely if $\mathfrak{H}$ is a transitive system and h_0 is in $\mathfrak{H}$ there is an S such that $k = h_0S$, $\mathfrak{H} = h_0\Gamma$.

We shall call a permutation group Γ a *transitive or intransitive group* according as $\mathfrak{G}$ itself is or is not a transitive system for Γ. When Γ is transitive we have $g\Gamma = \mathfrak{G}$ for every g of $\mathfrak{G}$. If Γ is intransitive every $g\Gamma$ is a proper subset of $\mathfrak{G}$.

3. Quasigroups. A set $\mathfrak{G}$ is said to form a quasigroup if a product

$$a \cdot x$$

is defined to be a unique element of $\mathfrak{G}$ for every a and x of $\mathfrak{G}$ such that the equations

$$(1) \qquad\qquad a \cdot x = b, \qquad y \cdot a = b$$

have unique solutions x and y for every a and b of $\mathfrak{G}$. Then every x of $\mathfrak{G}$ determines a transformation

---

(4) This term has a very different meaning in topology but its use here and in the theory of algebras seems very desirable.

$$R_x: \qquad\qquad g \rightarrow gR_x = g \cdot x$$

of $\mathfrak{G}$. If $aR_x = gR_x$ then $a \cdot x = g \cdot x$ and the second uniqueness hypothesis of (1) implies that $a = g$. Thus every R_x is a permutation of $\mathfrak{G}$. We shall call R_x a *right multiplication* of $\mathfrak{G}$ and shall designate by $\mathfrak{G}_r$ the set of all right multiplications of $\mathfrak{G}$. In general $\mathfrak{G}_r$ is a subset but not necessarily a subgroup of Σ.

In a similar fashion we determine the *left multiplications*

$$L_x: \qquad\qquad g \rightarrow gL_x = x \cdot g$$

of $\mathfrak{G}$. They are also permutations.

A quasigroup now consists of a set $\mathfrak{G}$ of elements g and a corresponding set $\mathfrak{G}_r$ of permutations R_g on $\mathfrak{G}$. The left multiplications L_g are then determined transformations and will be permutations if it is true that $gR_x = gR_y$ only if $x = y$. This requires that the correspondence $g \rightarrow R_y$ shall be one-to-one and that if two distinct permutations of $\mathfrak{G}_r$ be applied to the same element of $\mathfrak{G}$ the results shall be distinct. Conversely when these conditions are given $\mathfrak{G}$ will be a quasigroup. For $g \cdot k = gR$, $x = bL_g^{-1}$, $y = bR_g^{-1}$ are all uniquely determined elements of $\mathfrak{G}$ when every R_g and L_g is a nonsingular transformation.

Note that $gS = gT$ is possible for distinct permutations S and T on $\mathfrak{G}$ but that if $xS = xT$ for every x of $\mathfrak{G}$, where S and T are independent of x, then $S = T$. Note also that in the case where $\mathfrak{G}$ is a finite set of n elements $e_1 \cdots e_n$ we are stating that $\mathfrak{G}$ consists of these elements and n permutations $R_1 \cdots R_n$ on them such that if $x_iR_j = x_iR_k$ for *any* i then $j = k$.

4. Isotopy. Two quasigroups $\mathfrak{G}$ and $\mathfrak{G}^{(0)}$ are said to have the same order if there is a one-to-one correspondence $g \rightarrow g_0$ between them. In our general considerations there will be no loss of generality if we regard all quasigroups of the same order as consisting of the same elements and thus differing only in their right multiplications.

Any quasigroup $\mathfrak{G}$ now consists of a set $\mathfrak{M}$ of elements and a corresponding set $\mathfrak{G}_r$ of right multiplications. Let $\mathfrak{G}^{(0)}$ be a second quasigroup consisting of the same set of elements and a set $\mathfrak{G}_r$ of permutations R_x on $\mathfrak{M}$. Then we shall say that $\mathfrak{G}$ and $\mathfrak{G}^{(0)}$ are isotopic if there exist permutations A, B, C on $\mathfrak{M}$ such that

$$(2) \qquad\qquad R_x^{(0)} = AR_{xB}C.$$

This is equivalent to the definition of product (g, x) in $\mathfrak{G}^{(0)}$ in terms of that in $\mathfrak{G}$ by

$$(3) \qquad\qquad (g, x) = (gA \cdot xB)C.$$

Then $(x, g) = (xA \cdot gB)C$ and

$$(4) \qquad\qquad L_x^{(0)} = BL_{xA}C.$$

Note that if $\mathfrak{G}$ is given then the transformations R_x and L_x are products of

permutations and are permutations. Thus if $\mathfrak{G}$ is a quasigroup and we define $\mathfrak{G}^{(0)}$ by (3) the resulting isotope is a quasigroup. As in the theory of nonassociative algebras the relation of isotopy is an equivalence relation.

5. **Principal isotopes.** Two quasigroups $\mathfrak{G}$ and $\mathfrak{G}^{(0)}$ of the same order are said to be isomorphic if there exists a permutation P on their common set of elements such that $(gP, xP) = (g \cdot x)P$. Then $(gP^{-1} \cdot xP^{-1})P = (a, x)$ and, if we define $A = P^{-1}$, we see that the isomorphism of two quasigroups may be regarded as the instance

$$(5) \qquad R_x^{(0)} = A R_{xA} A^{-1}, \qquad L_x^{(0)} = A L_{xA} A^{-1}$$

of isotopy. Moreover we have

LEMMA 2. *Every isotope $\mathfrak{G}^{(1)}$ of a quasigroup $\mathfrak{G}$ is isomorphic to a principal isotope $\mathfrak{G}^{(0)}$ defined by*

$$(6) \qquad R_x^{(0)} = A R_{xB}, \qquad L_x^{(0)} = B L_{xA}.$$

For let $R_x^{(1)} = S R_{xT} U$. Then $\mathfrak{G}^{(1)}$ is isomorphic to $\mathfrak{G}^{(0)}$ defined by $R_x^{(0)} = U R_x^{(1)} U^{-1} = A R_{xB}$ where $A = US$, $B = UT$. The second formula of (6) follows from the consequence (4) of (2) in the case $C = I$.

Principal isotopes are more convenient to study than general isotopes and we shall use Lemma 2 frequently in our proofs.

6. **Loops.** A quasigroup $\mathfrak{G}$ is said to have an identity element e if $e \cdot x = x \cdot e = x$ for every x of $\mathfrak{G}$. Then $xR_e = xL_e = x$ for every x, and e is that unique element of $\mathfrak{G}$ such that $R_e = L_e$ is the identity transformation I. It will be very convenient to have a special name for such quasigroups and, as we said in our introduction, we shall call them loops.

We shall show that every quasigroup is isotopic to a loop. A construction of all loops will then yield quasigroups from which all quasigroups may be constructed. Thus it will be at least reasonable to restrict all further study to that of loops.

THEOREM 1. *Let f and g be any elements of a quasigroup $\mathfrak{G}$ so that there exists a unique h in $\mathfrak{G}$ such that $f = g \cdot h$. Then f is the identity element of the loop which is the principal isotope of $\mathfrak{G}$ defined by (6) with*

$$(7) \qquad A = R_h^{-1}, \qquad B = L_g^{-1}.$$

Conversely if a loop $\mathfrak{G}^{(0)}$ is a principal isotope of $\mathfrak{G}$ it is defined by (6) and (7) for elements g and h of $\mathfrak{G}$ such that $f = g \cdot h$ is the identity element of $\mathfrak{G}^{(0)}$.

For if $f = g \cdot h = g R_h = h L_g$ we may write $g = fA$, $h = fB$ for A and B of (7). Then $R_f^{(0)} = A R_{fB} = A R_h = I$, $L_f^{(0)} = B L_{fA} = B L_g = I$. Conversely if $\mathfrak{G}^{(0)}$ is defined by (6) and f is the identity element of $\mathfrak{G}^{(0)}$ then $R_f^{(0)} = A R_{fB} = L_f^{(0)} = B L_{fA} = I$. Put $g = fA$ and $h = fB$ to obtain (7) as well as $f = gA^{-1} = g R_h = g \cdot h$.

7. Groups. A quasigroup $\mathfrak{G}$ becomes a group when we assume the associative law $x\cdot(a\cdot y)=(x\cdot a)\cdot y$ for every a, x, y of $\mathfrak{G}$. Then $aR_yL_x=aL_xR_y$. Hence $\mathfrak{G}$ is a group if and only if $R_xL_y=L_yR_x$ for all right and left multiplications of $\mathfrak{G}$. It is known that the group property implies the existence of an identity element, that is, an associative quasigroup is always a loop. We also have

LEMMA 3. *A loop $\mathfrak{G}$ is a group if and only if $\mathfrak{G}_r$ is a group. Then $\mathfrak{G}$ and $\mathfrak{G}_r$ are isomorphic.*

For $x\rightarrow R_x$ is a one-to-one mapping of $\mathfrak{G}$ on $\mathfrak{G}_r$. If $\mathfrak{G}$ is a group we have $(a\cdot x)y=aR_xR_y=a\cdot(x\cdot y)=aR_{x\cdot y}$, $R_xR_y=R_{x\cdot y}$, our correspondence is an isomorphism, $\mathfrak{G}_r$ is a group. Conversely let $\mathfrak{G}$ be a loop with identity element e so that

$$(8) \qquad\qquad eR_x = eL_x = x$$

for every x of $\mathfrak{G}$. If $\mathfrak{G}_r$ is a group we have $R_xR_y=R_g$ where g is a uniquely determined element of $\mathfrak{G}$. For the permutations S of $\mathfrak{G}_r$ are in a one-to-one correspondence $S\rightarrow g$ with the elements g of $\mathfrak{G}$ such that $S=R_g$. But $eR_x\cdot eR_y =eR_x\cdot y=eR_xR_y=eR_g=g=x\cdot y$, $R_xR_y=R_{x\cdot y}$, $g\rightarrow R_g$ is an isomorphism of the group $\mathfrak{G}_r$ and $\mathfrak{G}$.

Note that in the case of an arbitrary loop we have $x\cdot y=eR_x\cdot eR_y=eR_xR_y =g=eR_g$, but we do not have $R_xR_y=R_g$. For R_xR_y may not even be in $\mathfrak{G}_r$.

We may now prove the important theorem:

THEOREM 2. *A loop is isotopic to a group if and only if it is isomorphic to the group and thus is itself a group.*

For let $\mathfrak{G}^{(0)}$ be a loop isotopic to a group $\mathfrak{G}$ so that we may assume $\mathfrak{G}^{(0)}$ to be a principal isotope of $\mathfrak{G}$ defined by (6), (7). Let e be the identity element of $\mathfrak{G}$, so that, if $y=x^{-1}$, $x\cdot y=e$, we have $R_{x\cdot y}=R_xR_y=I$, $R_y=R_x^{-1}$. Similarly $L_{x^{-1}}=(L_x)^{-1}$. Then $xB=xL_g^{-1}=xL_{g^{-1}}=g^{-1}\cdot x$, $xA=xR_h^{-1}=x\cdot h^{-1}$. But $f^{-1}=(g\cdot h)^{-1}=h^{-1}\cdot g^{-1}$ and

$$(9) \qquad\qquad R_x^{(0)} = R_h^{-1}R_{xB} = R_{f^{-1}\cdot x}.$$

Similarly $L_x^{(0)}=L_g^{-1}L_{xA}=L_{g^{-1}}L_{x\cdot h^{-1}}=L_{x\cdot f^{-1}}$. But then every $R_x^{(0)}$ is commutative with every $L_g^{(0)}$, $\mathfrak{G}^{(0)}$ is associative. By Lemma 3, $\mathfrak{G}$ and $\mathfrak{G}_r$ are isomorphic, $\mathfrak{G}_r^{(0)}=\mathfrak{G}_r$, $\mathfrak{G}$ and $\mathfrak{G}^{(0)}$ are isomorphic.

8. Subloops. The right multiplications R_h of the elements h of any subset $\mathfrak{H}$ of a loop $\mathfrak{G}$ generate a group of transformations which we shall designate by $\mathfrak{H}_\rho$. It consists of all finite products of positive, negative and zero integral powers of the transformations R_h for h in $\mathfrak{H}$. The left multiplications L_h also generate a transformation group $\mathfrak{H}_\lambda$, and the right and left multiplications

together a group $\mathfrak{H}_\tau$. All of these groups are subgroups of the group $\mathfrak{G}_\tau$ defined as above for $\mathfrak{H} = \mathfrak{G}$.

A subloop of a loop $\mathfrak{G}$ is a subset $\mathfrak{H}$ which forms a loop with respect to the defining operation of $\mathfrak{G}$. It is sufficient that $\mathfrak{H}$ form a quasigroup, that is, that $\mathfrak{H}$ contain all products $h \cdot k$ and the solutions x and y of $x \cdot h = k$, $h \cdot y = k$ taken when h and k are in $\mathfrak{H}$. For then $\mathfrak{H}$ will contain the solution e of $x \cdot h = h$. Thus *the identity element of a loop $\mathfrak{G}$ is the identity element of all of its subloops.*

LEMMA 4. *A set $\mathfrak{H}$ is a subloop of $\mathfrak{G}$ if and only if $e\mathfrak{H}_\tau = \mathfrak{H}$.*

For let $\mathfrak{H}$ be a subloop of $\mathfrak{G}$ so that $\mathfrak{H}$ contains $eI = e$. The elements of $\mathfrak{H}_\tau$ are products of transformations R_h, L_h, R_h^{-1}, L_h^{-1}, and if $k = eS$ is in $\mathfrak{H}$, then $e(SR_h) = k \cdot h$, $e(SL_h) = h \cdot k$, $x = (eS)R_h^{-1} = kR_h^{-1}$, $y = (eS)L_h^{-1} = kL_h^{-1}$ are all in $\mathfrak{H}$. Hence $e\mathfrak{H}_\tau$ is contained in $\mathfrak{H}$, every $h = eR_h$ is contained in $e\mathfrak{H}_\tau$, $e\mathfrak{H}_\tau = \mathfrak{H}$. Conversely if $e\mathfrak{H}_\tau = \mathfrak{H}$ we have $eR_hR_k = h \cdot k$ and the solutions $x = eR_kR_h^{-1}$, $y = eL_kL_h^{-1}$ of $x \cdot h = k$ and $h \cdot y = k$ in $\mathfrak{H}$. Then $\mathfrak{H}$ is a subloop.

It should be observed that the order of a subloop $\mathfrak{H}$ of a finite loop $\mathfrak{G}$ need not divide the order of $\mathfrak{G}$. For example let $\mathfrak{G}$ consist of $e = e_1$, e_2, e_3, e_4, e_5, and let $R_{e_i} = R_i$ be defined by $R_e = I$, $R_2 = (12)(345)$, $R_3 = (13)(254)$, $R_4 = (14)(235)$, $R_5 = (15)(243)$. Evidently $e_i \cdot e = e_iR_e = e_i$, $e \cdot e_i = eR_i = e_i$, e is the identity element of $\mathfrak{G}$. We compute $e_2 \cdot e_2 = e_1$, $e_2 \cdot e_3 = e_5$, $e_2 \cdot e_4 = e_3$, $e_2 \cdot e_5 = e_4$ so that $L_2(12)(354)$. By symmetry $L_3 = (13)(245)$, $L_4 = (14)(253)$, $L_5 = (15)(234)$ and $\mathfrak{G}$ is a loop. Its four subloops (e, e_i), defined for $i = 2, 3, 4, 5$, are all groups of order two.

9. Cosets. Every subgroup Γ of $\mathfrak{G}_\tau$ defines subsets $x\Gamma$ of $\mathfrak{G}$ which we shall call cosets of $\mathfrak{G}$ relative to Γ. They are transitive systems of Γ by Lemma 1. Thus every element of $\mathfrak{G}$ is in one and only one coset and the sets $x\Gamma$ provide a coset decomposition of $\mathfrak{G}$.

If $\mathfrak{H}$ is a subloop of a loop $\mathfrak{G}$ we shall call the cosets $x\mathfrak{H}_\rho$ the right-hand cosets of $\mathfrak{G}$ relative to $\mathfrak{H}$. Similarly, we shall call the cosets $x\mathfrak{H}_\lambda$ the left-hand cosets of $\mathfrak{G}$ relative to $\mathfrak{H}$, and the cosets $x\mathfrak{H}_\tau$ the two-sided cosets of $\mathfrak{G}$ relative to $\mathfrak{H}$.

The sets $x\mathfrak{H}$ consisting of all elements $x \cdot h$ for h in the subloop $\mathfrak{H}$ do not, in general, have the property that each element is in one and only one such set. For if $x \cdot h = y \cdot k$ then $y = xR_hR_k^{-1}$ is in $x\mathfrak{H}_\rho$ but may not be in $x\mathfrak{H}$. We shall not call such sets cosets. However, our definition of normal divisors will have the consequence $x\mathfrak{H}_\rho = x\mathfrak{H}_\tau = x\mathfrak{H}$.

With every subgroup Γ of $\mathfrak{G}$ and corresponding coset decomposition of $\mathfrak{G}$ we associate the set Γ^* of all transformations S of $\mathfrak{G}_\tau$ such that xS is in $x\Gamma$ for every x of $\mathfrak{G}$. Then $x\Gamma^*$ is contained in $x\Gamma$. But clearly Γ is contained in Γ^*, $x\Gamma$ is in $x\Gamma^*$, $x\Gamma = x\Gamma^*$ for every x. Also we have

LEMMA 5. *The sets Γ^* are subgroups of $\mathfrak{G}_\tau$.*

For if H and K are in Γ^* and x is in $\mathfrak{G}$ we have $y = xH = xS$ where S is

in Γ. Then $yK=yT$ where T is in Γ, $(xH)K=(xS)T$, $x(HK)=x(ST)=xU$ for $U=ST$ in Γ, HK is in Γ^*. Also $z=xH^{-1}$ has the property $zH=zS$ where S is in Γ if H is in Γ^*, $x=zS$, $x\Gamma=zS\Gamma=z\Gamma$ since Γ is a group, $S\Gamma=\Gamma$ if S is in Γ. Then $z=xH^{-1}$ is in $x\Gamma$ and H^{-1} is in Γ^*.

Note that every subloop $\mathfrak{H}$ of $\mathfrak{G}$ determines a unique subgroup $\mathfrak{H}_\rho^*$ of $\mathfrak{G}_r$ such that $e H_\rho^*=e\mathfrak{H}_\rho=\mathfrak{H}=e\mathfrak{H}_r$ by Lemma 3. However $\mathfrak{H}_r$ is not necessarily a subgroup of $\mathfrak{H}_\rho^*$.

10. Normal divisors. A homomorphism of a loop $\mathfrak{G}$ on a loop $\mathfrak{G}'$ is a mapping $g\rightarrow g'$ of $\mathfrak{G}$ on $\mathfrak{G}'$ such that every element of $\mathfrak{G}'$ is the image g' of an element g of $\mathfrak{G}$, and $(x\cdot y)'=x'\cdot y'$ for every x and y of $\mathfrak{G}$. The mapping $x\rightarrow x\mathfrak{H}_\rho$ of $\mathfrak{G}$ on the quotient set $\mathfrak{G}/\mathfrak{H}$ of all cosets $x\mathfrak{H}_\rho$ satisfies the first of these properties. We shall call a subloop $\mathfrak{H}$ of $\mathfrak{G}$ a *normal divisor* of $\mathfrak{G}$ if $\mathfrak{G}/\mathfrak{H}$ is a loop and $x\rightarrow x\mathfrak{H}_\rho$ is a homomorphism of $\mathfrak{G}$ on $\mathfrak{G}/\mathfrak{H}$.

The hypothesis that $\mathfrak{G}/\mathfrak{H}$ is a loop implies that either of the equations

$$(10) \qquad x\mathfrak{H}_\rho\cdot y\mathfrak{H}_\rho = x\mathfrak{H}_\rho\cdot w\mathfrak{H}_\rho, \qquad y\mathfrak{H}_\rho\cdot x\mathfrak{H}_\rho = w\mathfrak{H}_\rho\cdot x\mathfrak{H}_\rho$$

is true if and only if $y\mathfrak{H}_\rho=w\mathfrak{H}_\rho$. The homomorphism hypothesis implies that

$$(11) \qquad x\mathfrak{H}_\rho\cdot y\mathfrak{H}_\rho = (x\cdot y)\mathfrak{H}_\rho,$$

and thus defines the product operation in $\mathfrak{G}/\mathfrak{H}$. Conversely (11) and (10) imply that $\mathfrak{G}/\mathfrak{H}$ is a loop and that $x\rightarrow x\mathfrak{H}_\rho$ is a homomorphism of $\mathfrak{G}$ on $\mathfrak{G}/\mathfrak{H}$. For $\mathfrak{H}=e\mathfrak{H}_\rho$ and by (11), we have $\mathfrak{H}\cdot y\mathfrak{H}_\rho=y\mathfrak{H}_\rho$, $x\mathfrak{H}_\rho\cdot \mathfrak{H}=x\mathfrak{H}_\rho$, $\mathfrak{H}$ is the identity element of $\mathfrak{G}/\mathfrak{H}$. Also $g\mathfrak{H}_\rho\cdot y\mathfrak{H}_\rho=(g\cdot y)\mathfrak{H}_\rho=b\mathfrak{H}_\rho$ and $x\mathfrak{H}_\rho\cdot g\mathfrak{H}_\rho=(x\cdot g)\mathfrak{H}_\rho=b\mathfrak{H}_\rho$ are satisfied by $y=bL_g^{-1}$, $x=bR_g^{-1}$ and the corresponding coset solutions are unique by (10). Then $\mathfrak{G}/\mathfrak{H}$ is a loop as desired.

Note that if

$$(12) \qquad \Gamma = \mathfrak{H}_\rho^*, \qquad \mathfrak{H} = e\Gamma, \qquad x\mathfrak{H}_\rho = x\Gamma$$

for every x, and (11) becomes

$$(13) \qquad x\Gamma\cdot y\Gamma = (x\cdot y)\Gamma.$$

Also we may use (11) to write (10) in the form

$$(14) \qquad (x\cdot y)\Gamma = (w\cdot y)\Gamma, \qquad (y\cdot x)\Gamma = (y\cdot w)\Gamma$$

if and only if $x\Gamma=w\Gamma$. We are now in a position to prove the fundamental theorem:

THEOREM 3. *A subset $\mathfrak{H}$ of a loop $\mathfrak{G}$ with identity element e is a normal divisor of $\mathfrak{G}$ if and only if $\mathfrak{H}=e\Gamma$ where Γ is a normal divisor of $\mathfrak{G}_r$. Then $\Gamma^*=\mathfrak{H}_\rho^*$ is also a normal divisor of $\mathfrak{G}_r$ and*

$$(15) \qquad x\Gamma = x\mathfrak{H}_\rho = x\mathfrak{H} = x\mathfrak{H}_\lambda = x\mathfrak{H}_r$$

for every x.

For let $\mathfrak{H}$ be a normal divisor of $\mathfrak{G}$ and define $\Gamma = \mathfrak{H}_\rho^*$ so that we have (12), (13), (14). Since every permutation of $\mathfrak{G}$ is a finite product of permutations R_g, R_g^{-1}, L_g, L_g^{-1} the group Γ will be a normal divisor of $\mathfrak{G}_r$ if we can show that $T^{-1}\Gamma T$ is contained in Γ for $T = R_g$, R_g^{-1}, L_g, L_g^{-1}. Now for every x and y of $\mathfrak{G}$ and S of Γ we define $w = xR_y SR_y^{-1}$ so that $xR_y S = wR_y$, $(x \cdot y)\Gamma = (w \cdot y)\Gamma$. By (14), $x\Gamma = w\Gamma$, w is in $x\Gamma$. But our definition of $\mathfrak{H}_\rho^*$ implies that $R_y SR_y^{-1}$ is in Γ, $R_y \Gamma R_y^{-1}$ is contained in Γ. Similarly define $w = xL_y SL_y^{-1}$ and obtain $(y \cdot x)S = y \cdot w$, $(y \cdot x)\Gamma = (y \cdot w)\Gamma$, $w\Gamma = x\Gamma$, w is in $x\Gamma$ and $L_y \Gamma L_y^{-1}$ is contained in Γ. We next put $z = xR_y^{-1}$ and have $z \cdot y = x$, $zS \cdot y = (z \cdot y)U$ where U is in Γ by (13). Then $xR_y^{-1}SR_y = xU$ is in $x\Gamma$ and $R_y^{-1}\Gamma R_y$ is contained in Γ. A similar argument with $z = yL_x^{-1}$ yields $x \cdot zS = (x \cdot z)U$, $yL_x^{-1}SL_x = yU$ and implies that $L_x^{-1}\Gamma L_x$ is contained in Γ, $\Gamma = \mathfrak{H}_\rho^*$ is a normal divisor of $\mathfrak{G}_r$.

Conversely let $\mathfrak{H} = e\Gamma$ where Γ is a normal divisor of $\mathfrak{G}_r$. If S and T are in Γ then $eS \cdot eT = eSR_{eT} = eR_{eT}U = eTU$ where U is in Γ, TU is in Γ. Also, $eS \cdot y = eT$ implies that $eSR_y = eR_y U = eT$, $y = eTU^{-1}$ is a unique element of $\mathfrak{H}$. Similarly $x \cdot eS = eSL_x = eL_x U = xU = eT$ has the unique solution $x = eTU^{-1}$ in $\mathfrak{H}$. Thus $\mathfrak{H}$ is a subloop of $\mathfrak{G}$. Now $xS \cdot yT = xSR_{yT} = xR_{yT}U = (x \cdot yT)U = yTR_x U = yL_x VU = (x \cdot y)VU$ where V and U are in Γ. Hence $x\Gamma \cdot y\Gamma$ is contained in $(x \cdot y)\Gamma$. But if S is in Γ we may determine $U = R_y SR_y^{-1}$ and have $(x \cdot y)S = xR_y S = xUR_y = xU \cdot y$, $(x \cdot y)\Gamma$ is contained in $x\Gamma \cdot y\Gamma$ and we have (13). If $(x \cdot y)\Gamma = (x \cdot w)\Gamma$ then $yL_x\Gamma = wL_x\Gamma$. But $L_x\Gamma = \Gamma L_x$ and $y\Gamma = w\Gamma$ as desired. Similarly $(y \cdot x)\Gamma = (w \cdot x)\Gamma$ and $yR_x\Gamma = wR_x\Gamma$, $y\Gamma = w\Gamma$. Now $xS = eL_x S = eUL_x = hL_x = x \cdot h$ where $h = eU$ is in $\mathfrak{H}$ and so $x\Gamma$ is contained in $x\mathfrak{H}$. Also $x \cdot h = x \cdot eS = eSL_x = eL_x U = xU$ for U in Γ, $x\mathfrak{H} = x\Gamma$. It follows that Γ^* contains every R_h. Similarly $h \cdot x = eSR_x = eR_x U = xU = xL_h$, Γ^* contains every L_h, Γ^* contains $\mathfrak{H}_r$, $x\Gamma^* = x\Gamma$ contains $x\mathfrak{H}_r$ which contains $x\mathfrak{H} = x\Gamma$. This gives (15). But $x\mathfrak{H}_\rho = x\Gamma$ and $\Gamma^* = \mathfrak{H}_\rho^*$, $x\Gamma = x\mathfrak{H}_\rho^*$ and we have (13) and (14) for Γ replaced by $\mathfrak{H}_\rho^*$. This proves our theorem.

It should be observed that there may be several normal divisors Γ of $\mathfrak{G}_r$ such that $\mathfrak{H} = e\Gamma$ is the same normal divisor of $\mathfrak{G}$. Indeed $\mathfrak{H} = e\Gamma = e\Delta$ if and only if $\mathfrak{H}$ is a transitive system of both Γ and Δ.

As an expected consequence of our definitions we now have

THEOREM 4. *Let $g \rightarrow g'$ be a homomorphism of a loop $\mathfrak{G}$ on a loop $\mathfrak{G}'$ and $\mathfrak{H}$ be the set of all elements h of $\mathfrak{G}$ such that h' is the identity element e' of $\mathfrak{G}'$. Then $\mathfrak{H}$ is a normal divisor of $\mathfrak{G}$ and the correspondence $x\mathfrak{H} \rightarrow x'$ is an isomorphism of the quotient loop $\mathfrak{G}/\mathfrak{H}$ and $\mathfrak{G}'$.*

For if h and k are in $\mathfrak{H}$ we have $(h \cdot k)' = h' \cdot k' = e'$ and $h \cdot k$ is in $\mathfrak{H}$. Also $x \cdot h = k$ implies that $x' \cdot h' = k'$, $x' = e'$, x is in $\mathfrak{H}$. Similarly $h \cdot y = k$ implies y is in $\mathfrak{H}$ and that $\mathfrak{H}$ is a subloop of $\mathfrak{G}$. The elements y of $x\mathfrak{H}_r$ are products of x by a finite number of elements h of $\mathfrak{H}$ with some order and grouping. Since every $h' = e'$ we have $y' = x'$ no matter what the order and grouping.

Conversely if $y' = x'$ we may write $y = x \cdot z$ for z in $\mathfrak{G}$ and $y' = x' \cdot z' = x'$. But $\mathfrak{G}'$ is a loop and $z' = e'$, z is in $\mathfrak{H}$, y is in $x\mathfrak{H}$. It follows that $x\mathfrak{H}_\tau \leqq x\mathfrak{H}$ and, since $x\mathfrak{H}_\tau \geqq x\mathfrak{H}_\rho \geqq x\mathfrak{H}$, then

$$x\mathfrak{H}_\tau = x\mathfrak{H}_\rho = x\mathfrak{H}_\lambda = x\mathfrak{H}.$$

Moreover $x' = y'$ implies that $x\mathfrak{H}_\rho = y\mathfrak{H}_\rho$, so that the correspondence $x\mathfrak{H} \rightarrow x'$ is one-to-one. We compute $[(x \cdot h) \cdot (y \cdot k)]' = (x \cdot h)' \cdot (y \cdot k)' = x' \cdot y' = (x \cdot y)'$ for every h and k of $\mathfrak{H}$ and see that $x\mathfrak{H} \cdot y\mathfrak{H} = (x \cdot y)\mathfrak{H}$. Conversely $(x \cdot y) \cdot h = x \cdot z$ has a solution z in $\mathfrak{G}$ which may be written in the form $z = y \cdot w$ for w in $\mathfrak{G}$. Then $[x \cdot (y \cdot w)]' = x' \cdot (y \cdot w)' = x' \cdot (y' \cdot w') = [(x \cdot y) \cdot h]' = x' \cdot y'$, $y' = y' \cdot w'$, $w' = e'$, w is in $\mathfrak{H}$, $(x \cdot y)\mathfrak{H} = x\mathfrak{H} \cdot y\mathfrak{H}$. This proves that $x\mathfrak{H} \rightarrow x'$ is an isomorphism of $\mathfrak{G}/\mathfrak{H}$ and the loop $\mathfrak{G}'$. Then $\mathfrak{G}/\mathfrak{H}$ is a loop and $\mathfrak{H}$ is a normal divisor of $\mathfrak{G}$.

11. The multiplications of quotient loops. If $\mathfrak{H}$ is a normal divisor of $\mathfrak{G}$ and $\Gamma = \mathfrak{H}_\rho{}^*$, the elements of $\mathfrak{G}/\mathfrak{H}$ are the cosets $x\Gamma$. The elements of $\mathfrak{G}_\tau/\Gamma$ are the cosets $S\Gamma = \Gamma S$ for S in $\mathfrak{G}_\tau$. Each such coset defines a transformation

$$(16) \qquad\qquad g\Gamma \rightarrow (g\Gamma)(S\Gamma) = (gS)\Gamma.$$

But if $aS\Gamma = gS\Gamma$ we have $a\Gamma S = g\Gamma S$, $a\Gamma = g\Gamma$. Hence (16) is a permutation of $\mathfrak{G}/\mathfrak{H}$. We may identify the permutation (16) with $S\Gamma$ and have shown that the elements of the quotient group $\mathfrak{G}_\tau/\Gamma$ may be regarded as being permutations of the quotient loop $\mathfrak{G}/\mathfrak{H}$.

The right multiplications of $\mathfrak{G}/\mathfrak{H}$ are the permutations

$$g\Gamma \rightarrow g\Gamma \cdot x\Gamma = (g\Gamma)(R_x\Gamma),$$

that is, the permutations $R_x\Gamma$ of $\mathfrak{G}_\tau/\Gamma$. Similarly the left multiplications of $\mathfrak{G}/\mathfrak{H}$ are the permutations $L_x\Gamma$. The group $\mathfrak{G}_\tau$ is generated by the right and left multiplications and thus $\mathfrak{G}_\tau/\Gamma$ is generated by the $R_x\Gamma$ and $L_y\Gamma$. But these permutations also generate the group of permutations for $\mathfrak{G}/\mathfrak{H}$.

THEOREM 5. *Let $\mathfrak{H}$ be a normal divisor of $\mathfrak{G}$ so that $\Gamma = \mathfrak{H}_\rho{}^*$ is a normal divisor of $\mathfrak{G}_\tau$. Then $(\mathfrak{G}/\mathfrak{H})_\tau = \mathfrak{G}_\tau/\Gamma$.*

12. Finite loops. In our proof of Theorem 3 we showed that the hypothesis $x\Gamma \cdot y\Gamma = (x \cdot y)\Gamma$ implies that $S^{-1}\Gamma S$ is contained in Γ for every S which is either a right multiplication or a left multiplication. In the case where $\mathfrak{G}$ is finite so is Γ and a comparison of orders then yields $S^{-1}\Gamma S = \Gamma$, $\Gamma = S\Gamma S^{-1}$. Indeed it is true that in the finite case if we have $S^{-1}\Gamma S \leqq \Gamma$, for elements S which generate $\mathfrak{G}_\tau$, the group Γ will be a normal divisor of $\mathfrak{G}_\tau$. Thus we have

THEOREM 6. *Let $\mathfrak{H}$ be a subloop of a finite loop $\mathfrak{G}$ and define $x' = x\mathfrak{H}_\rho$ for every x of $\mathfrak{G}$. Then if $(x \cdot y)' = x' \cdot y'$ for every x and y of $\mathfrak{G}$ the quotient set $\mathfrak{G}/\mathfrak{H}$ is a loop and $\mathfrak{H}$ is a normal divisor of $\mathfrak{G}$.*

We may also prove

THEOREM 7. *The order of a normal divisor $\mathfrak{H}$ of a finite loop $\mathfrak{G}$ divides the order of $\mathfrak{G}$.*

For if $\mathfrak{H}$ is a normal divisor of $\mathfrak{G}$ we have seen that every element x of $\mathfrak{G}$ is in one and only one set $x\mathfrak{H}$. If $x \cdot h = x \cdot k$ then $h = k$ so that each coset $x\mathfrak{H}$ has exactly as many elements as does $\mathfrak{H}$. Then the order of $\mathfrak{G}$ is the product of the order of $\mathfrak{H}$ and the order of $\mathfrak{G}/\mathfrak{H}$.

This result evidently implies that if a finite loop $\mathfrak{G}$ is homomorphic to a loop $\mathfrak{G}'$ the order of $\mathfrak{G}'$ divides the order of $\mathfrak{G}$.

13. **Simple loops.** A subgroup Γ of $\mathfrak{G}_r$ defines a proper subset $e\Gamma$ of $\mathfrak{G}$ if and only if Γ is intransitive. As in the theory of groups we call a loop simple if its only proper normal divisor is the identity group. Then we have

THEOREM 8. *A loop $\mathfrak{G}$ is simple if and only if the group $\mathfrak{G}_r$ has no intransitive normal divisor except the identity group.*

Every isotope of a loop $\mathfrak{G}$ is isomorphic to a principal isotope $\mathfrak{G}^{(0)}$ of $\mathfrak{G}$. If the original isotope is a loop so is $\mathfrak{G}^{(0)}$ and we may let f be the identity element of $\mathfrak{G}^{(0)}$. Theorem 1 implies that $\mathfrak{G}_r^{(0)} \leqq \mathfrak{G}_r$. The relation of principal isotopy is symmetric and thus $\mathfrak{G}_r = \mathfrak{G}_r^{(0)}$. We pass to a loop $\mathfrak{G}^{(1)}$ isomorphic to $\mathfrak{G}^{(0)}$ and defined by

$$R_x^{(1)} = C R_{xc}^{(0)} C^{-1}, \qquad L_x = C L_{xc}^{(0)} C^{-1}$$

with $C = R_f^{-1}$. Then $\mathfrak{G}^{(1)}$ has e as its identity element. Moreover $\mathfrak{G}_r^{(1)} = C G_r^{(0)} C^{-1} = \mathfrak{G}_r^{(0)} = \mathfrak{G}_r$ since C is in $\mathfrak{G}_r$. The application of Theorem 3 yields

THEOREM 9. *Every loop isotopic to a loop $\mathfrak{G}$ is isomorphic to a loop having precisely the same normal divisors as $\mathfrak{G}$.*

Note that we are not stating that the normal divisors $e\Gamma$ of $\mathfrak{G}^{(1)}$ are isomorphic or even isotopic to the normal divisors of $\mathfrak{G}$. They merely consist of the same elements. If $\mathfrak{H} = e\Gamma$ then multiplication for $\mathfrak{H}$ in $\mathfrak{G}$ is defined by $y \cdot h = y R_h$ and in $\mathfrak{G}^{(1)}$ by $(y, h) = y C A R_{hBC} C^{-1}$. It does not appear necessary for $\mathfrak{H}$ in $\mathfrak{G}$ and in $\mathfrak{G}_r$ to be isotopic.

As a consequence of Theorem 9 we have

THEOREM 10. *All loops isotopic to a simple loop are simple.*

14. **Centers.** The *center* $\mathfrak{C}$ of a loop $\mathfrak{G}$ is the set of all quantities c of $\mathfrak{G}$ such that the commutative and associative laws for products hold whenever c is one of the factors. The condition $x \cdot (y \cdot c) = (x \cdot y) \cdot c$ is equivalent to $R_c L_x = L_x R_c$ for every x, and $c \cdot (x \cdot y) = (c \cdot x) \cdot y$ yields $L_c R_y = R_y L_c$ for every c. But $x \cdot c = c \cdot x$ is equivalent to $L_c = R_c$. Hence every R_c is in the center Λ of the group $\mathfrak{G}_r$, every $c = e R_r$, $\mathfrak{C} = e\Lambda$.

Suppose now that H is in Λ and that $c = eH$. Then $x \cdot c = c L_x = eH L_x = e L_x H = xH$, $H = R_c$. Similarly $c \cdot x = c R_x = eH R_x = e R_x H = xH$, $L_c = R_c$. We also have

$R_cL_x = L_xR_c$ so that $x \cdot (y \cdot c) = (x \cdot y) \cdot c$ and similarly $c \cdot (x \cdot y) = (c \cdot x) \cdot y$. But then $R_{y \cdot c} = R_yR_c = R_cR_y = R_{c \cdot y}$ and $(x \cdot c) \cdot y = x \cdot (c \cdot y)$, $c = eH$ is in $\mathfrak{C}$. Hence $\mathfrak{C} = e\Lambda$.

The correspondence $c \to H = R_c$ is one-to-one since if H is given then $c = eH$. Also $eH \cdot eK = eHR_{eK} = eHK$ for every H and K of Λ. Thus we have

THEOREM 11. *The center $\mathfrak{C}$ of a loop $\mathfrak{G}$ with identity element e is isomorphic to the center Λ of $\mathfrak{G}_r$, and $\mathfrak{C} = e\Lambda$.*

If $\mathfrak{G}$ and $\mathfrak{G}^{(0)}$ are loops which are principal isotopes the group $\mathfrak{G}_r = \mathfrak{G}_r^{(0)}$ and the centers of $\mathfrak{G}$ and $\mathfrak{G}^{(0)}$ are isomorphic. By Lemma 2 we have

THEOREM 12. *Isotopic loops have isomorphic centers.*

15. Homotopy. While it has been convenient to define isotopy for algebraic systems consisting of the same elements it is not, of course, necessary. Thus we may define two multiplicative algebraic systems $\mathfrak{G}$ and $\mathfrak{G}'$ to be isotopic if there exist nonsingular mappings A, B, C of $\mathfrak{G}$ on $\mathfrak{G}'$ such that

$$(17) \qquad\qquad xA \cdot yB = (x \cdot y)C.$$

The concept of homomorphism may now be generalized. We call two mappings A and B of a set $\mathfrak{G}$ on a set $\mathfrak{G}' = \mathfrak{G}A = \mathfrak{G}B$ *equivalent* if there exists a nonsingular transformation N of $\mathfrak{G}$ and a nonsingular transformation S of $\mathfrak{G}'$ such that

$$B = NAS.$$

Then we shall say that a multiplicative system $\mathfrak{G}$ is *homotopic* to a multiplicative system $\mathfrak{G}'$ if there exist equivalent mappings A, B, C on $\mathfrak{G}$ to $\mathfrak{G}'$ such that $\mathfrak{G}' = \mathfrak{G}C$ and (17) holds for all x and y of $\mathfrak{G}$. Then $A = NCS$, $B = QCT$, $xNCS \cdot yQCT = (x \cdot y)C$. Define $(x', y') = x'S \cdot y'T$ for every x' and y' of $\mathfrak{G}'$ and $(x, y) = xN^{-1} \cdot yQ^{-1}$ to obtain $(xC, yC) = (x, y)C$. The argument is readily reversed and we see that $\mathfrak{G}$ *is homotopic to* $\mathfrak{G}'$ *if and only if an isotope of $\mathfrak{G}$ is homomorphic to an isotope of* $\mathfrak{G}'$.

We note now that $\mathfrak{G}$ is itself homomorphic to an isotope of $\mathfrak{G}'$ if there exists a mapping P of $\mathfrak{G}$ on $\mathfrak{G}'$ and nonsingular transformations S, T, U of $\mathfrak{G}$ such that $\mathfrak{G}' = \mathfrak{G}P$ and $(xP, yP) = (x \cdot y)P$ where $(x', y') = (x'S \cdot y'T)U$. This is equivalent to (17) with $A = PS$, $B = PT$, $C = PU^{-1}$. Then $A = C(US)$, $B = P(CT)$. Hence (17) implies that $\mathfrak{G}$ is homomorphic to an isotope of $\mathfrak{G}'$ if there exist nonsingular transformations S and T of $\mathfrak{G}'$ such that $A = CS$, $B = CT$. However such transformations may not exist.

For example let $\mathfrak{G}$ be any group of at least three distinct elements and C be any singular mapping of $\mathfrak{G}$ on a set $\mathfrak{G}'$ of at least two distinct elements. Then there exist distinct elements g, h, k in $\mathfrak{G}$ such that $gC = hC$, $gC \neq kC$. The transformation N on $\mathfrak{G}$ which interchanges h and k and leaves all other elements of $\mathfrak{G}$ unaltered is nonsingular and we define a homotopy of $\mathfrak{G}$ on $\mathfrak{G}'$

with $A = B = NC$. This defines the product operation in $\mathfrak{G}'$ and is such that $gN = g$, $gNC = gC \neq kN = hNC$. However if $A = CS$ we could conclude from $gC = hC$ that $gCS = hCS$, $gA = hA$, a contradiction.

Let us observe that if we designate the right and left multiplications of $\mathfrak{G}'$ respectively by $R_{xA}^{(1)}$ and $L_{yB}^{(1)}$ then (17) is equivalent to $xAR_{yB}^{(1)} = xR_yC$, $yBL_{xA}^{(1)} = yL_xC$ and thus to

$$(18) \qquad\qquad AR_{yB}^{(1)} = R_yC, \qquad BL_{xA}^{(1)} = L_xC.$$

We assume that $\mathfrak{G}$ is a loop homotopic to a loop $\mathfrak{G}'$ and let e be the identity element of $\mathfrak{G}$. Replace x and y in (18) by e to obtain

$$C = AR_{eB}^{(1)} = BL_{eA}^{(1)}.$$

Since $\mathfrak{G}'$ is a loop both $R_{eB}^{(1)}$ and $L_{eA}^{(1)}$ are nonsingular transformations on $\mathfrak{G}'$ and $\mathfrak{G}$ is homomorphic to the isotope $\mathfrak{G}''$ of $\mathfrak{G}'$ defined by $(x', y') = x'S \cdot y'T$ where $S^{-1} = R_{eB}^{(1)}$, $T^{-1} = L_{eA}^{(1)}$. Since $(xC, yC) = (x \cdot y)C$ we see that eC is the identity element of $\mathfrak{G}''$ and $\mathfrak{G}''$ is a loop. We have proved

THEOREM 13. *Let a loop $\mathfrak{G}$ be homotopic to a loop $\mathfrak{G}'$. Then $\mathfrak{G}$ is homomorphic to a loop isotopic to $\mathfrak{G}'$.*

If $\mathfrak{H}$ is the normal divisor of $\mathfrak{G}$ which is mapped by C on eC the quotient loop $\mathfrak{G}/\mathfrak{H}$ is isotopic to $\mathfrak{G}'$. We note also that we have the almost immediate

COROLLARY. *Let a group $\mathfrak{G}$ be homotopic to a loop $\mathfrak{G}'$. Then $\mathfrak{G}$ is homomorphic to $\mathfrak{G}'$ and $\mathfrak{G}'$ is a group.*

For by Theorem 13 the group $\mathfrak{G}$ is homomorphic to $\mathfrak{G}''$, $\mathfrak{G}''$ is a group isotopic to $\mathfrak{G}'$, $\mathfrak{G}''$ is isomorphic to $\mathfrak{G}'$ by Theorem 2.

16. **Special loops.** A loop $\mathfrak{G}$ may be called *alternative* if the conditions

$$R_g^{-1} = R_{g^{-1}}, \qquad L_g^{-1} = L_{g^{-1}}, \qquad R_gL_gR_x = R_{g \cdot x}L_g, \qquad R_gL_{g \cdot x} = L_xR_gL_g$$

hold for every g and x of $\mathfrak{G}$ where $g \cdot g^{-1} = g^{-1} \cdot g = e$ is the identity element of $\mathfrak{G}$. Then it is known[5] that every two elements of $\mathfrak{G}$ generate a subloop which is a group.

An example of such a loop is given by the nonzero elements of the non-associative Cayley-Dickson division algebra of order eight over the field of all real numbers. This loop contains a finite loop $\mathfrak{G}$ of sixteen elements. It consists of eight basal elements $e_1 = 1$, e_2, $\cdots$, e_7 and their negatives and $e_i(e_je_k) = \pm(e_ie_j)e_k$. The algebra is a central simple algebra and thus the center $\mathfrak{C}$ of the knot $\mathfrak{G}$ consists of the group of two elements 1, -1. Evidently the

(5) See R. Moufang, *Struktur von Alternativkorpern*, Math. Ann. vol. 110 (1935) pp. 416–430, for a discussion showing that this set of postulates imply that every two elements of the loop generate a group. The postulates are given also in the Hausman-Ore paper on page 993.

quotient loop $\mathfrak{G}/\mathfrak{C}$ is the abelian group of exponent two and order eight. This is important as an example of a case where $\mathfrak{H}$ is a group and $\mathfrak{G}/\mathfrak{H}$ is a group but $\mathfrak{G}$ is a loop which is not associative.

The theory of alternative loops is only one of many interesting questions about loops suggested by topics of the theory of nonassociative algebras. For example, the construction of new simple algebras recently[6] given by the author yields, by the use of basal units, a construction of what may be called a crossed extension $\mathfrak{B}$ of every finite loop $\mathfrak{A}$, in which $\mathfrak{A}$ is a normal divisor of $\mathfrak{B}$, and the quotient loop $\mathfrak{B}/\mathfrak{A}$ is a prescribed permutation group on $\mathfrak{A}$ leaving its identity element unaltered. The study of other properties of such loops should prove to be of considerable interest.

---

[6] *Non-associative algebras.* II. *New simple algebras*, Ann. of Math. vol. 43 (1942) pp. 708–723.

THE UNIVERSITY OF CHICAGO,
    CHICAGO, ILL.