QUASIGROUPS. II

BY

A. A. ALBERT

1. **Introduction.** In the first part(1) of this paper we associated every quasigroup $\mathfrak{G}$ with the transformation group $\mathfrak{G}_\tau$ generated by the right and left multiplications of $\mathfrak{G}$. We defined isotopy and showed that every quasigroup is isotopic to a loop, that is, a quasigroup $\mathfrak{G}$ with identity element e. We also defined the concept of normal divisor for all loops and showed that every normal divisor $\mathfrak{H}$ of $\mathfrak{G}$ is equal to $e\Gamma$ where Γ is a normal divisor of $\mathfrak{G}_\tau$.

The main purpose of this second part of our paper is that of presenting a proof, using the results above, of the Schreier refinement theorem and the consequent Jordan-Hölder theorem for arbitrary loops. We obtain also a number of special results, among them a construction(2) of all loops $\mathfrak{G}$ with a given normal divisor $\mathfrak{H}$ and a given quotient loop $\mathfrak{G}/\mathfrak{H}$. We use this in the construction of all loops of order six with a subloop, necessarily a normal divisor, of order three. We classify these loops into nonisotopic classes and show also that all quasigroups of order five are isotopic to one of two nonisotopic loops.

2. **Normal divisors of subloops.** The right multiplications R_h of the elements h of a subset $\mathfrak{H}$ of a loop $\mathfrak{G}$ generate a group $\mathfrak{H}_\rho$, the left multiplications L_h a group $\mathfrak{H}_\lambda$, and all R_h and L_h a group $\mathfrak{H}_\tau$. These groups are all subgroups of the transformation group $\mathfrak{G}_\tau$.

We let $\mathfrak{H}$ be a subset of a subloop $\mathfrak{A}$ of $\mathfrak{G}$. Then $\mathfrak{H}_\rho \subset \mathfrak{A}_\rho$, $\mathfrak{H}_\lambda \subset \mathfrak{A}_\lambda$. Hence $\mathfrak{H}_\rho$, $\mathfrak{H}_\lambda$, $\mathfrak{H}_\tau$ are all subgroups of $\mathfrak{A}_\tau$. The cosets

$$a\mathfrak{H}_\rho \qquad (a \text{ in } \mathfrak{A})$$

are all subsets of $\mathfrak{A}$. We define

$$\mathfrak{H}_\mathfrak{A}$$

to be the set of all transformations S of $\mathfrak{A}_\tau$ such that aS is in $a\mathfrak{H}_\rho$ for every a of $\mathfrak{A}$. Then $(aS)T = a(ST) = (aS)U = aVU$ for V and U in $\mathfrak{H}_\rho$, VU is in $\mathfrak{H}_\rho$, $a(ST)$ is in $a\mathfrak{H}_\rho$. If $aST^{-1} = b$ then $aS = bT = bU = aV$, $b = aVU^{-1}$ is in $a\mathfrak{H}_\rho$. It follows that $\mathfrak{H}_\mathfrak{A}$ is a subgroup of $\mathfrak{A}_\tau$(3).

A subloop $\mathfrak{H}$ of $\mathfrak{G}$ is a normal divisor of $\mathfrak{G}$ if the cosets $x\mathfrak{H}_\rho$ form a loop

Presented to the Society, November 27, 1943; received by the editors October 11, 1943.

(1) *Quasigroups.* I, Trans. Amer. Math. Soc. vol. 54 (1943) pp. 507–519.

(2) In a recent letter R. H. Bruck indicated that he had obtained the same construction several months before I did. He did not, however, formulate the notion of associated extension sets which we give here. In view of the fact that Bruck's construction has not yet been published, that I obtained the results independently, and that I apply them in the study of loops of order six I felt it desirable to retain the construction in the present paper.

(3) In *Quasigroups.* I, we stated and proved this result only in the case $\mathfrak{A} = \mathfrak{G}$.

$\mathfrak{G}/\mathfrak{H}$ and the mapping $x \to x\mathfrak{H}_\rho$ is a homomorphism of $\mathfrak{G}$ on $\mathfrak{G}/\mathfrak{H}$. Then we have shown([4]) that $\mathfrak{H}$ is a normal divisor of $\mathfrak{G}$ if and only if $\mathfrak{H}_\mathfrak{G}$ is a normal divisor of $\mathfrak{G}_\tau$. The proof of this result may be carried through without a word of change to yield

LEMMA 1. *Let $\mathfrak{A}$ be a subloop of $\mathfrak{G}$. A subset $\mathfrak{H}$ of $\mathfrak{A}$ is a normal divisor of $\mathfrak{A}$ if and only if $\mathfrak{H} = e\Gamma$ where Γ is a normal divisor of $\mathfrak{A}_\tau$. Then $\mathfrak{H}_\mathfrak{A}$ is a normal divisor of $\mathfrak{A}_\tau$ and $x\mathfrak{H}_\mathfrak{A} = x\mathfrak{H}$ for every x of $\mathfrak{A}$.*

Our definition of normal divisor is sometimes inconvenient to apply and may be sharpened to yield

LEMMA 2. *A subloop $\mathfrak{H}$ of a loop $\mathfrak{G}$ is a normal divisor of $\mathfrak{G}$ if and only if*

$$(1) \qquad (x\mathfrak{H})(y\mathfrak{H}) \subset (xy)\mathfrak{H}, \qquad x\mathfrak{H} \subset (x\mathfrak{H})h, \qquad (xy)\mathfrak{H} \subset x(y\mathfrak{H})$$

for all x, y of $\mathfrak{G}$ and h of $\mathfrak{H}$. Then

$$(2) \qquad (x\mathfrak{H})(y\mathfrak{H}) = (xy)\mathfrak{H} = (xh)(y\mathfrak{H}) = (x\mathfrak{H})(yh),$$

or all x, y of $\mathfrak{G}$ and h of $\mathfrak{H}$.

For $(x\mathfrak{H})\mathfrak{H} \subset x\mathfrak{H}$ and so $x(ST)$ is in $x\mathfrak{H}$ for all right multiplications S and T of elements of $\mathfrak{H}$. If z is in $x\mathfrak{H}$ and $S = R_h$ we have z in $(x\mathfrak{H})S$, zS^{-1} is in $x\mathfrak{H}$. The right multiplications of the elements of $\mathfrak{H}$ and their inverses generate the group $\mathfrak{H}_\rho$ and so $x\mathfrak{H}_\rho \subset x\mathfrak{H}$, $x\mathfrak{H}_\rho = x\mathfrak{H}$. Also $(xy)\mathfrak{H} \subset x(y\mathfrak{H}) \subset (x\mathfrak{H})(y\mathfrak{H}) \subset (xy)\mathfrak{H}$ so that $(x\mathfrak{H})(y\mathfrak{H}) = x(y\mathfrak{H}) = (xy)\mathfrak{H}$. If $(x\mathfrak{H})(y\mathfrak{H}) = (x\mathfrak{H})(w\mathfrak{H})$ then $(xy)\mathfrak{H} = (xw)\mathfrak{H}$, xw is in $(xy)\mathfrak{H} = x(y\mathfrak{H})$, $xw = x(yh)$, $w = yh$, $w\mathfrak{H} = (yh)\mathfrak{H} = y(h\mathfrak{H}) = y\mathfrak{H}$. Thus $\mathfrak{H}$ satisfies our definition of a normal divisor.

Conversely let $\mathfrak{H}$ be a normal divisor of $\mathfrak{G}$ so that $x\mathfrak{H} = x\Gamma$ where Γ is a normal divisor of $\mathfrak{G}_\tau$ containing $\mathfrak{H}_\rho$. Then $(xh)(y\mathfrak{H}) \subset (x\mathfrak{H})(y\mathfrak{H}) = (xy)\mathfrak{H}$. But $(xh)(y\mathfrak{H}) = y\Gamma L_{xh} = (yL_{xh})\Gamma = [(xh)y]\Gamma = (xR_hR_y)\Gamma = (xR_y)U\Gamma = (xy)\Gamma = (xy)\mathfrak{H}$ where $R_y^{-1}R_hR_y = U$ in Γ. Similarly $(x\mathfrak{H})(yh) = x\Gamma R_{yh} = xR_{yh}\Gamma = [x(yh)]\Gamma(yR_hL_x)\Gamma = (xy)U\Gamma = (xy)\Gamma = (xy)\mathfrak{H}$.

It should be noted that (1) and $x\mathfrak{H} = \mathfrak{H}x$ are formal consequences of (2) since $\mathfrak{G}$ has an identity element e. We now use Lemma 2 to prove

LEMMA 3. *Let $\mathfrak{H} = e\Gamma$ be a subloop of a subloop $\mathfrak{A}$ of $\mathfrak{G}$ and Γ be a subloop of $\mathfrak{G}_\tau$ such that*

$$R_x\Gamma R_x^{-1} = L_x\Gamma L_x^{-1} = \Gamma$$

for every x of $\mathfrak{A}$. Then $\mathfrak{H}$ is a normal divisor of $\mathfrak{A}$.

For $x\mathfrak{H} = x(e\Gamma) = e\Gamma L_x = eL_x\Gamma = x\Gamma$ for every x of $\mathfrak{A}$. If S and T are in Γ then $(xS)(yT) = xSR_{yT} = xR_{yT}U = [x(yT)]U = [(yT)L_x]U = (yL_x)(VU)$ where V and U are in Γ. Then $(x\Gamma)(y\Gamma) \subset (xy)\Gamma$. Also $(x\Gamma)h = x\Gamma R_h = xR_h\Gamma = xh\Gamma$

([4]) *Quasigroups*. I, Theorem 3.

$= [x(eS)]\Gamma = [e(SL_x)]\Gamma = (eL_x)U\Gamma = x\Gamma$ since U is in Γ, $U\Gamma = \Gamma$. Finally $x(y\Gamma) = y\Gamma L_x = yL_x\Gamma = (xy)\Gamma$ and we have (1).

Note that we are not assuming that Γ is a subgroup of $\mathfrak{A}_r$ nor even that Γ contains $\mathfrak{H}_\rho$. The hypotheses of this lemma are satisfied if $\mathfrak{H}$ is a normal divisor of $\mathfrak{G}$ and we have, as a consequence,

LEMMA 4. *If $\mathfrak{H}$ is a normal divisor of $\mathfrak{G}$ it is a normal divisor of every subloop $\mathfrak{A}$ of $\mathfrak{G}$ which contains it.*

The result also follows directly from Lemma 2.

3. **Intersections.** The *intersection* of any two subsets $\mathfrak{B}$ and $\mathfrak{C}$ of a loop $\mathfrak{G}$ is the set

$$\mathfrak{D} = \mathfrak{B} \cap \mathfrak{C}$$

of all elements of $\mathfrak{G}$ which are in both $\mathfrak{B}$ and $\mathfrak{C}$. It is a trivial task to verify that if $\mathfrak{B}$ and $\mathfrak{C}$ are subloops of $\mathfrak{G}$ then $\mathfrak{D}$ is a subloop of $\mathfrak{B}$, of $\mathfrak{C}$, of $\mathfrak{G}$.

Define $\Delta_\rho = \mathfrak{B}_\rho \cap \mathfrak{C}_\rho$, $\Delta_\lambda = \mathfrak{B}_\lambda \cap \mathfrak{C}_\lambda$, $\Delta_\tau = \mathfrak{B}_\tau \cap \mathfrak{C}_\tau$. Then we have

LEMMA 5. *Let $\mathfrak{B}$ and $\mathfrak{C}$ be subloops of $\mathfrak{G}$ and $\mathfrak{D} = \mathfrak{B} \cap \mathfrak{C}$. Then $\mathfrak{D}_\rho \subset \Delta_\rho$, $\mathfrak{D}_\lambda \subset \Delta_\lambda$, $\mathfrak{D}_\tau \subset \Delta_\tau$, $\mathfrak{D} = e\Delta_\rho = e\Delta_\lambda = e\Delta_\tau$.*

For d is in $\mathfrak{D}$ if and only if R_d is in $\mathfrak{B}_\rho$ and in $\mathfrak{C}_\rho$, R_d is in Δ_ρ. Hence $\mathfrak{D}_\rho \subset \Delta_\rho$, $e\mathfrak{D}_\rho = \mathfrak{D} \subset e\Delta_\rho$. But $e\Delta_\rho \subset \mathfrak{B}$, $e\Delta_\rho \subset \mathfrak{C}$ so that $e\Delta_\rho \subset \mathfrak{D}$, $e\Delta_\rho = \mathfrak{D}$. The remaining properties are proved similarly.

If $\mathfrak{H}$ and $\mathfrak{K}$ are normal divisors of $\mathfrak{G}$ then $x\mathfrak{H} = x\mathfrak{H}_\mathfrak{G}$, $x\mathfrak{K} = x\mathfrak{K}_\mathfrak{G}$ for every x of $\mathfrak{G}$. The intersection Δ of $\mathfrak{H}_\mathfrak{G}$ and $\mathfrak{K}_\mathfrak{G}$ is a normal divisor of $\mathfrak{G}_r$ and thus $e\Delta$ is a normal divisor of $\mathfrak{G}$. But $e\Delta \subset \mathfrak{H}$, $e\Delta \subset \mathfrak{K}$ so that $e\Delta \subset \mathfrak{D}$ where $\mathfrak{D} = \mathfrak{H} \cap \mathfrak{K}$. Let $\Delta_r = \mathfrak{H}_r \cap \mathfrak{K}_r$. Then $e\Delta \supset e\Delta_r = \mathfrak{D}$ by Lemma 5 and we have proved the standard

THEOREM 1. *The intersection of two normal divisors of a loop $\mathfrak{G}$ is a normal divisor of $\mathfrak{G}$.*

If $\mathfrak{A}$ is a subloop of $\mathfrak{G}$ and $\mathfrak{H}$ is a normal divisor of $\mathfrak{G}$ the intersection Δ of $\mathfrak{A}_r$ and $\mathfrak{H}_\mathfrak{G}$ is a normal divisor of $\mathfrak{A}_r$. By Lemma 1 the loop $e\Delta$ is a normal divisor of $\mathfrak{A}$. As in the proof of Lemma 5 we have $(\mathfrak{H} \cap \mathfrak{A}) = e\Delta$. We form the cosets $a\mathfrak{H}$ for a in $\mathfrak{A}$ and see that if a and b are in $\mathfrak{A}$ and $ab = c$ then $(a\mathfrak{H})(b\mathfrak{H}) = c\mathfrak{H}$. If a and c are in $\mathfrak{A}$ we determine b in $\mathfrak{A}$ such that $ab = c$ and see that $(a\mathfrak{H})(x\mathfrak{H}) = b\mathfrak{H}$ has the solution $x = c$. Similarly if $ya = b$ then $(y\mathfrak{H})(a\mathfrak{H}) = b\mathfrak{H}$. But then

$$\mathfrak{L} = \mathfrak{A}\mathfrak{H} \tag{3}$$

is a subloop of $\mathfrak{G}$, $\mathfrak{H}$ is a normal divisor of $\mathfrak{L}$. If $a\mathfrak{H} = b\mathfrak{H}$ then $b = ad$ where d is in $\mathfrak{H}$, d is in $\mathfrak{A}$, d is in $\mathfrak{D} = \mathfrak{H} \cap \mathfrak{A}$. Thus $a\mathfrak{H} = b\mathfrak{H}$ if and only if $a\mathfrak{D} = b\mathfrak{D}$. The mapping $a\mathfrak{H} \to a\mathfrak{D}$ is thus one-to-one and clearly defines an isomorphism of $\mathfrak{A}\mathfrak{H}/\mathfrak{H}$ and $\mathfrak{A}/\mathfrak{D}$. Every $x\mathfrak{H} = \mathfrak{H}x$, $\mathfrak{L} = \mathfrak{H}\mathfrak{A}$, and we have

THEOREM 2. *Let $\mathfrak{A}$ be a subloop of $\mathfrak{G}$, $\mathfrak{H}$ be a normal divisor of $\mathfrak{G}$. Then the intersection $\mathfrak{D}$ of $\mathfrak{H}$ and $\mathfrak{A}$ is a normal divisor of $\mathfrak{A}$, $\mathfrak{L}=\mathfrak{A}\mathfrak{H}=\mathfrak{H}\mathfrak{A}$ is a subloop of $\mathfrak{G}$ such that*

$$\mathfrak{L}/\mathfrak{H} \cong \mathfrak{A}/\mathfrak{D}. \tag{4}$$

If $\mathfrak{D}$ is the identity group, $a\mathfrak{H}=b\mathfrak{H}$ if and only if $a=b$. Since two cosets are equal if and only if they have an element in common we have the

COROLLARY. *Let the intersection of a subloop $\mathfrak{A}$ and a normal divisor $\mathfrak{H}$ of $\mathfrak{G}$ be the identity loop. Then either of the equations*

$$ah = bk, \quad ha = kb \qquad (a, b \text{ in } \mathfrak{A};\ h, k \text{ in } \mathfrak{H})$$

is true if and only if $a=b$, $h=k$.

4. **Unions.** The *union* of two subsets $\mathfrak{B}$ and $\mathfrak{C}$ of a loop $\mathfrak{G}$ is the intersection of all subloops of $\mathfrak{G}$ which contain both $\mathfrak{B}$ and $\mathfrak{C}$. Since $\mathfrak{G}$ is such a subloop the union of $\mathfrak{B}$ and $\mathfrak{C}$ is a subloop of $\mathfrak{G}$. It contains $\mathfrak{B}$ and $\mathfrak{C}$ and so contains $\mathfrak{B}\mathfrak{C}$. It follows trivially that we have

LEMMA 6. *Let $\mathfrak{B}$ and $\mathfrak{C}$ be subloops of $\mathfrak{G}$. Then their union is $\mathfrak{B}\mathfrak{C}$ if and only if $\mathfrak{B}\mathfrak{C}$ is a subloop of $\mathfrak{G}$.*

If $\mathfrak{H}$ and $\mathfrak{K}$ are normal divisors of $\mathfrak{G}$ the union Γ of $\mathfrak{H}_{\mathfrak{G}}$ and $\mathfrak{K}_{\mathfrak{G}}$ is a normal divisor of $\mathfrak{G}_r$, $e\Gamma$ is a normal divisor of $\mathfrak{G}$. Then $e\Gamma$ contains $\mathfrak{H}$ and $\mathfrak{K}$ and so contains their union. But $\Gamma=\mathfrak{H}_{\mathfrak{G}}\mathfrak{K}_{\mathfrak{G}}$, $e\Gamma=e\mathfrak{H}_{\mathfrak{G}}\mathfrak{K}_{\mathfrak{G}}=\mathfrak{H}\mathfrak{K}_{\mathfrak{G}}=\mathfrak{H}\mathfrak{K}$, $\mathfrak{L}=\mathfrak{H}\mathfrak{K}=e\Gamma$. We have proved

THEOREM 3. *The union of two normal divisors $\mathfrak{H}$ and $\mathfrak{K}$ of $\mathfrak{G}$ is the normal divisor $\mathfrak{H}\mathfrak{K}$ of $\mathfrak{G}$.*

A subloop $\mathfrak{H}$ of $\mathfrak{G}$ is a maximal normal divisor of $\mathfrak{G}$ if and only if $\mathfrak{G}/\mathfrak{H}$ is simple. Indeed, as for groups, we may apply Lemma 2 to see that every normal divisor $\mathfrak{A}$ of $\mathfrak{G}$ such that $\mathfrak{A}\supset\mathfrak{H}$ arises from a normal divisor $\mathfrak{A}_0$ of $\mathfrak{G}/\mathfrak{H}$ such that $\mathfrak{A}_0=\mathfrak{A}/\mathfrak{H}$. If $\mathfrak{H}$ and $\mathfrak{K}$ are normal divisors of $\mathfrak{G}$ which are distinct and maximal their union $\mathfrak{L}=\mathfrak{H}\mathfrak{K}$ contains $\mathfrak{H}$ properly and, by Theorem 3, $\mathfrak{L}=\mathfrak{G}$. We apply Theorem 2 to see that $\mathfrak{L}/\mathfrak{H}\cong\mathfrak{K}/\mathfrak{D}$ so that $\mathfrak{K}/\mathfrak{D}$ is simple, $\mathfrak{D}$ is a maximal normal divisor of $\mathfrak{G}$. Thus we have

THEOREM 4. *Let $\mathfrak{H}$ and $\mathfrak{K}$ be distinct maximal normal divisors of a loop $\mathfrak{G}$ and $\mathfrak{D}$ be their intersection. Then $\mathfrak{D}$ is a maximal normal divisor of $\mathfrak{H}$ and of $\mathfrak{K}$ such that*

$$\mathfrak{G}/\mathfrak{H} \cong \mathfrak{K}/\mathfrak{D}, \qquad \mathfrak{G}/\mathfrak{K} \cong \mathfrak{H}/\mathfrak{D}. \tag{5}$$

5. **The Jordan-Hölder theorem.** The result of Theorem 4 is sufficient to carry through the proof of the Jordan-Hölder theorem for finite loops exactly as in the classical case of groups. The proof of the result for infinite loops by

the Schreier refinement theorem requires a more delicate analysis. We first prove

LEMMA 7. *Let $\mathfrak{H}$ be a normal divisor of $\mathfrak{G}$, $\mathfrak{C}_0$ be a normal divisor of a subloop $\mathfrak{C}$ of $\mathfrak{G}$. Then $\mathfrak{C}_0\mathfrak{H}$ is a normal divisor of $\mathfrak{C}\mathfrak{H}$.*

For, by Theorem 2 and Lemma 6, $\mathfrak{C}\mathfrak{H}$ is the union of $\mathfrak{C}$ and $\mathfrak{H}$ and is a subloop of $\mathfrak{G}$, $\mathfrak{C}_0\mathfrak{H}$ is a subloop of $\mathfrak{C}\mathfrak{H}$. If c is in $\mathfrak{C}$ and h is in $\mathfrak{H}$ then $ch(\mathfrak{C}_0\mathfrak{H}) = (c\mathfrak{C}_0)\mathfrak{H} = c(\mathfrak{C}_0\mathfrak{H})$ by the use of Lemma 2. If also c_1 is in $\mathfrak{C}$ and h_1 is in $\mathfrak{H}$ we have $[(ch)(\mathfrak{C}_0\mathfrak{H})][(c_1h_1)(\mathfrak{C}_0\mathfrak{H})] = [(c\mathfrak{C}_0)\mathfrak{H}][(c_1\mathfrak{C}_0)\mathfrak{H}] = [(c\mathfrak{C}_0)(c_1\mathfrak{C}_0)]\mathfrak{H} = [(cc_1)\mathfrak{C}_0]\mathfrak{H} = (cc_1)(\mathfrak{C}_0\mathfrak{H})$, $[(ch)(c_1h_1)](\mathfrak{C}_0\mathfrak{H}) = [(cc_1)h']\mathfrak{C}_0\mathfrak{H} = [(cc_1)\mathfrak{C}_0]\mathfrak{H} = (cc_1)(\mathfrak{C}_0\mathfrak{H})$ as desired. Also $(ch)[(c_1h_1)(\mathfrak{C}_0\mathfrak{H})] = (ch)[c_1(\mathfrak{C}_0\mathfrak{H})] = (ch)[(c_1\mathfrak{C}_0)\mathfrak{H}] = [c(c_1\mathfrak{C}_0)]\mathfrak{H} = [(cc_1)\mathfrak{C}_0]\mathfrak{H} = (cc_1)(\mathfrak{C}_0\mathfrak{H})$ and we have the third relation of (1). Finally $[(ch)(\mathfrak{C}_0\mathfrak{H})](c_0h_1) = [(c\mathfrak{C}_0)]\mathfrak{H}(c_0h_1) = [(c\mathfrak{C}_0)c_0]\mathfrak{H} = (c\mathfrak{C}_0)\mathfrak{H} = (ch)\mathfrak{C}_0\mathfrak{H}$. This proves our lemma.

If $\mathfrak{C}_0$ is a normal divisor of a subloop $\mathfrak{C}$ of $\mathfrak{G}$ then $\mathfrak{C}_0 = e\Gamma$ where Γ is a normal divisor of $\mathfrak{C}_\tau$. Let $\mathfrak{B}$ be a subloop of $\mathfrak{G}$ and $\Delta = \mathfrak{B}_\tau \cap \Gamma$. Then $e\Delta \subset e\mathfrak{B}_\tau = \mathfrak{B}$, $e\Delta \subset \mathfrak{C}_0$, $e\Delta \subset (\mathfrak{B}\cap\mathfrak{C}_0)$. But $\Delta \supset \Delta_\rho$ and, by Lemma 5, $e\Delta = (\mathfrak{B}\cap\mathfrak{C}_0)$. The loop $\mathfrak{B}\cap\mathfrak{C}$ consists of elements a with R_a and L_a in $\mathfrak{B}_\tau\cap\mathfrak{C}_\tau$ and, by the associative case of the lemma below, Δ is a normal divisor of $\mathfrak{B}_\tau\cap\mathfrak{C}_\tau$. By Lemma 3 we have

LEMMA 8. *Let $\mathfrak{B}$ and $\mathfrak{C}$ be subloops of $\mathfrak{G}$ and $\mathfrak{C}_0$ be a normal divisor of $\mathfrak{C}$. Then $\mathfrak{B}\cap\mathfrak{C}_0$ is a normal divisor of $\mathfrak{B}\cap\mathfrak{C}$.*

Our result now follows as in the associative case from

THEOREM 5. *Let $\mathfrak{B}$ and $\mathfrak{C}$ be subloops of $\mathfrak{G}$, $\mathfrak{B}_0$ be a normal divisor of $\mathfrak{B}$, $\mathfrak{C}_0$ be a normal divisor of $\mathfrak{C}$. Then*

$$(6) \qquad (\mathfrak{B}\cap\mathfrak{C})\mathfrak{B}_0/(\mathfrak{B}\cap\mathfrak{C}_0)\mathfrak{C}_0 \cong (\mathfrak{C}\cap\mathfrak{B})\mathfrak{C}_0/(\mathfrak{C}\cap\mathfrak{B}_0)\mathfrak{C}_0.$$

For, by Lemma 8, $\mathfrak{B}\cap\mathfrak{C}_0$ is a normal divisor of $\mathfrak{A} = \mathfrak{B}\cap\mathfrak{C}$ and, by Lemma 7, $\mathfrak{H} = (\mathfrak{B}\cap\mathfrak{C}_0)\mathfrak{B}_0$ is a normal divisor of the subloop $\mathfrak{L} = \mathfrak{A}\mathfrak{B}_0$ of $\mathfrak{B}$. But $\mathfrak{A}\mathfrak{H} = [(\mathfrak{B}\cap\mathfrak{C})\mathfrak{B}_0][(\mathfrak{B}\cap\mathfrak{C}_0)\mathfrak{B}_0] = [(\mathfrak{B}\cap\mathfrak{C})(\mathfrak{B}\cap\mathfrak{C}_0)]\mathfrak{B}_0$ by (1), $\mathfrak{A}\mathfrak{H} = \mathfrak{A}\mathfrak{B}_0$ since $\mathfrak{A}(\mathfrak{B}\cap\mathfrak{C}_0) = \mathfrak{A}$. Hence $\mathfrak{L} = \mathfrak{A}\mathfrak{H}$. We apply Theorem 2 to obtain $\mathfrak{L}/\mathfrak{H} \cong \mathfrak{A}/\mathfrak{D}$ where $\mathfrak{D}$ is the intersection of $\mathfrak{A}$ and $\mathfrak{H}$. If d is in $(\mathfrak{B}\cap\mathfrak{C}_0)(\mathfrak{B}_0\cap\mathfrak{C})$ then d is in $\mathfrak{A}$ and in $\mathfrak{H}$, d is in $\mathfrak{D}$. Conversely if $d = d_0b_0$ where d_0 is in $\mathfrak{B}\cap\mathfrak{C}_0$ and b_0 is in $\mathfrak{B}_0$ then d is in $\mathfrak{B}\cap\mathfrak{C}$ if and only if b_0 is in $\mathfrak{B}\cap\mathfrak{C}$, b_0 is in $\mathfrak{B}_0\cap\mathfrak{C}$. But then $\mathfrak{D} = (\mathfrak{B}_0\cap\mathfrak{C}_0)(\mathfrak{B}_0\cap\mathfrak{C})$. By symmetry

$$(\mathfrak{C}\cap\mathfrak{B})\mathfrak{C}_0/(\mathfrak{C}\cap\mathfrak{B}_0)\mathfrak{C}_0 \cong \mathfrak{C}\cap\mathfrak{B}/(\mathfrak{C}\cap\mathfrak{B}_0)(\mathfrak{C}_0\cap\mathfrak{B}).$$

However $(\mathfrak{C}\cap\mathfrak{B}_0)(\mathfrak{C}_0\cap\mathfrak{B}) = (\mathfrak{B}\cap\mathfrak{C}_0)(\mathfrak{B}_0\cap\mathfrak{C})$ and our theorem is proved.

This result implies the usual refinement theory(5) implying that the *composition loops* $\mathfrak{G}_{i-1}/\mathfrak{G}_i$ in any two *composition* series $\mathfrak{G}_0 \supset \mathfrak{G}_1 \supset \mathfrak{G}_2 \supset \cdots \supset \mathfrak{G}_r = [I]$ of $\mathfrak{G} = \mathfrak{G}_0$ may be ordered so that corresponding members are isomor-

(5) Cf. H. Zassenhaus, *Lehrbuch der Gruppentheorie*, Leipzig, 1937.

phic. It would be interesting to determine the validity of the conjecture that a loop $\mathfrak{G}$ has a composition series if and only if $\mathfrak{G}_r$ has a composition series. We leave this as an open question.

As in the theory of groups with operators we define an *operator S of a loop* $\mathfrak{G}$ to be a homomorphism of $\mathfrak{G}$ on a subloop $\mathfrak{G}S$ of $\mathfrak{G}$. If $\mathfrak{M}$ is any set of operators on $\mathfrak{G}$ we call $\mathfrak{G}$ an $\mathfrak{M}$-loop and define $\mathfrak{M}$-allowable subloop and normal $\mathfrak{M}$-divisor in the usual fashion. The refinement theory for $\mathfrak{M}$-loops then follows almost exactly as for groups and we do not feel that it would have been worth while to encumber our proofs with the additional necessary details.

6. **Loop extensions.** Let $\mathfrak{H}$ be a loop with identity element e and Λ be a loop with identity element I. We propose to construct a class of loops to one of which every loop $\mathfrak{G}$ with $\mathfrak{H}$ as a normal divisor, and $\mathfrak{G}/\mathfrak{H}$ isomorphic to Λ, is isomorphic.

We begin with a one-to-one mapping

$$S \rightarrow j_S \qquad (S \text{ in } \Lambda)$$

of Λ on a set of elements j_S such that

$$j_I = e.$$

Define $j_I \cdot h = h$ for every h of $\mathfrak{H}$ and $j_S \cdot e = j_S$ for every S of Λ. Adjoin as further elements the formal products $j_S \cdot h$ for every $h \neq e$ of $\mathfrak{H}$ and $S \neq I$ of Λ. Assume also that $j_S \cdot h = j_T \cdot k$ if and only if $S = T$ and $h = k$. The set $\mathfrak{G}$ of all formal products $j_S \cdot h$ now contains $\mathfrak{H}$ as well as the elements j_S.

Let ϕ be a set of functions

$$\phi_{S,T}(h, k)$$

on $\mathfrak{H}\mathfrak{H}$ to $\mathfrak{H}$ such that ϕ contains a uniquely defined function $\phi_{S,T}$ for every pair S, T of elements of Λ. We define $\mathfrak{H}_{S,T}$ to be the algebraic system consisting of the elements of $\mathfrak{H}$ and the operation $\phi_{S,T}$, and assume that every $\mathfrak{H}_{S,T}$ is a quasigroup. Moreover we assume that every $\mathfrak{H}_{S,I}$ is a loop with identity element e and that e is a left identity of every $\mathfrak{H}_{I,T}$. Finally let $\mathfrak{H}_{I,I} = \mathfrak{H}$, that is, $\phi_{I,I}(h, k) = hk$.

Define multiplication in $\mathfrak{G}$ by

$$(j_S \cdot h)(j_T \cdot k) = j_{ST}\phi_{S,T}(h, k). \tag{7}$$

We shall call $\mathfrak{G}$ the *crossed extension of* $\mathfrak{G}$ *by* Λ *relative to the extension set* ϕ, and write

$$\mathfrak{G} = (\mathfrak{H}, \Lambda, \phi).$$

By (7) we have $hk = (j_I \cdot h)(j_I \cdot k) = j_I\phi_{I,I}(h, k)$ and the products in $\mathfrak{G}$ of the elements of $\mathfrak{H}$ coincide with their products in $\mathfrak{H}$. Thus if $\mathfrak{G}$ is a loop the loop $\mathfrak{H}$ is a subloop of $\mathfrak{G}$. We note that $e = j_I \cdot e$, $e(j_T \cdot k) = j_I \cdot \phi_{I,T}(e, k) = j_I \cdot k$ since e is a left identity of $\mathfrak{H}_{I,T}$. Similarly $(j_S \cdot h)e = j_S \cdot \phi_{S,I}(h, e) = j_S \cdot h$ and e is the iden-

tity element of $\mathfrak{G}$. Observe also that $j_S h = (j_S \cdot e)(j_I \cdot h) = j_I \cdot \phi_{S,I}(e, h) = j_S \cdot h$ and our formal products $j_S \cdot h$ are the actual products $j_S h$ in $\mathfrak{G}$. Thus $\mathfrak{G}$ has been decomposed into the mutually exclusive sets $j_S \mathfrak{H}$. We shall prove

THEOREM 6. *Every crossed extension $\mathfrak{G} = (\mathfrak{H}, \Lambda, \phi)$ is a loop with $\mathfrak{H}$ as a normal divisor and $\mathfrak{G}/\mathfrak{H}$ isomorphic to Λ. Conversely every loop $\mathfrak{G}$ containing a normal divisor $\mathfrak{H}$ is a crossed extension of $\mathfrak{H}$ by $\Lambda = \mathfrak{G}/\mathfrak{H}$.*

The unverified conditions that $\mathfrak{G}$ be a loop are that the equations

$$ax = b, \qquad ya = b$$

shall have *unique* solutions x and y in $\mathfrak{G}$ for every a and b in $\mathfrak{G}$. Put $a = j_S h$, $b = j_U w$, $x = j_T k$ and use (7) to see that $ax = b$ if and only if $ST = U$, $\phi_{S,T}(h, k) = w$. Since Λ is a loop there is a unique solution T of $ST = U$. Each $\mathfrak{H}_{S,T}$ is a quasigroup and there is a unique solution k of $\phi_{S,T}(h, k) = w$. Similarly we write $y = j_R v$ and have $RS = U$ for R uniquely determined in Λ, $w = \phi_{R,S}(v, h)$ has a unique solution v in $\mathfrak{H}_{R,S}$. This proves that $\mathfrak{G}$ is a loop with $\mathfrak{H}$ as a subloop.

Equation (7) also implies that the correspondence $j_S h \to S$ is preserved under multiplication. It then is a homomorphism of $\mathfrak{G}$ and Λ in which $x \to I$ if and only if x is in $\mathfrak{H}$. It follows that $\mathfrak{H}$ is a normal divisor of $\mathfrak{G}$ and that $\mathfrak{G}/\mathfrak{H}$ is isomorphic to Λ.

Assume next that a loop $\mathfrak{H}$ is a normal divisor of a loop $\mathfrak{G}$ and take $\Lambda = \mathfrak{G}/\mathfrak{H}$. We define $j_I = e$. Every coset $S = x\mathfrak{H}$ of Λ contains elements not in any coset $T \neq S$ and the selection of an arbitrary element $x = j_S$ in each $S \neq \mathfrak{H}$ implies that $S = j_S \mathfrak{H}$. Then $ST = (j_S \mathfrak{H})(j_T \mathfrak{H}) = (j_S j_T)\mathfrak{H}$, $(j_S h)(j_T k) = j_{ST} w$ where $w = \phi_{S,T}(h, k)$ is a uniquely determined element of $\mathfrak{H}$. Thus $\mathfrak{H}_{S,T}$ is a multiplicative system. Now $(j_S h)e = j_S \phi_{S,I}(h, e) = j_S h$ so that $\phi_{S,I}(h, e) = h$. Similarly $e(j_T k) = j_T k$ and $\phi_{I,T}(e, k) = k$. Also $j_S h = (j_S e)(j_I h) = j_S \phi_{S,I}(e, h)$ and $h = \phi_{S,I}(e, h)$. We have proved that e is the identity element of every $\mathfrak{H}_{S,I}$ and is a left identity of every $\mathfrak{H}_{I,T}$. Clearly $\mathfrak{H}_{I,I} = \mathfrak{H}$. If S, T, h, w are given every solution k of $\phi_{S,T}(h, k) = w$ determines a unique solution $x = j_T k$ of $(j_S h)x = j_{ST} w$ and conversely. But $\mathfrak{G}$ is a loop and our former equation must have a unique solution. Similarly the existence of a unique solution h of $\phi_{S,T}(h, k) = w$ follows from the existence of a unique solution of $y\,(j_T k) = j_{ST} w$. Thus each $\mathfrak{H}_{S,T}$ is a quasigroup, $\mathfrak{G} = (\mathfrak{H}, \Lambda, \phi)$ for ϕ the set of all our $\phi_{S,T}$.

It is important for us to observe that the quasigroups $\mathfrak{H}_{S,T}$ *are entirely independent.* This property is *not* a property of *group* extensions.

Illustrations of crossed extensions are easily obtained by selecting each of the quasigroups $\mathfrak{H}_{S,T}$ to be an isotope of $\mathfrak{H}$. Then

$$\phi_{S,T}(h, k) = [(hA_{S,T})(kB_{S,T})]C_{S,T}$$

where the permutations $A_{S,T}$, $B_{S,T}$, $C_{S,T}$ are arbitrary except that $A_{S,I}$, $B_{S,I}$,

$C_{S,I}$ must be restricted so that e is the identity element of $\mathfrak{H}_{S,I}$, and $A_{I,T}$, $B_{I,T}$, $C_{I,T}$ must be restricted so that e is a left identity of $\mathfrak{H}_{I,T}$.

7. **Associated extension sets.** The element j_S in the coset $S=j_S\mathfrak{H}$ was taken to be any element of this coset except that $j_I=e$. If we replace j_S by

$$y_S = j_S c_S, \qquad y_I = j_I,$$

we have $S=y_S\mathfrak{H}$ and

$$\mathfrak{G} = (\mathfrak{H}, \Lambda, \phi) = (\mathfrak{H}, \Lambda, \psi) \tag{8}$$

for an extension set ψ to be determined. We shall call ϕ and ψ *associated*(6) extension sets and see that the equality (8) holds if and only if ϕ and ψ are associated.

The element c_S in $\mathfrak{H}$ determines a left multiplication $h\to\phi_{S,I}(c_S, h)$ in $\mathfrak{H}_{S,I}$ which we shall designate by L_S. Then

$$y_S h = (j_S c_S)(j_I h) = j_S(hL_S).$$

It follows that $(y_S h)(y_T k) = [j_S(hL_S)][j_T(kL_T)] = j_{ST}\phi(hL_S, kL_T) = y_{ST}\psi_{S,T}(h, k)$ $= j_{S,T}[\psi_{S,T}(h, k)L_{ST}]$. Hence ψ is associated with ϕ if and only if

$$\psi_{S,T}(h, k) = [\phi_{S,T}(hL_S, kL_T)]L_{ST}^{-1}. \tag{9}$$

Note that L_I is the identity transformation.

We observe that the quasigroups $\mathfrak{H}^{(0)}_{S,T}$ defined by the functions $\psi_{S,T}$ are isotopes of the corresponding $\mathfrak{H}_{S,T}$. In particular each

$$\psi_{S,I}(h, k) = hL_S R_k^{(S)} L_S^{-1} = hQ_k^{(S)}$$

where $R_k^{(S)}$ is the right multiplication defined for k in $\mathfrak{H}_{S,I}$, $Q_k^{(S)}$ is the right multiplication defined for k in $\mathfrak{H}^{(0)}_{S,I}$,

$$Q_k^{(S)} = L_S R_k^{(S)} L_S^{-1}.$$

Then $\mathfrak{H}^{(0)}_{S,I}$ has right multiplications conjugate to those of $\mathfrak{H}_{S,I}$ in the total transformation group. The loop $\mathfrak{H}^{(0)}_{S,I}$ is isomorphic to $\mathfrak{H}_{S,I}$ if $\mathfrak{H}_{S,I}$ is a group.

The fact that e is an identity of every $\mathfrak{H}^{(0)}_{S,I}$ and a left identity of every $\mathfrak{H}^{(0)}_{I,T}$ follows from Theorem 1. To verify these results directly from (7) we note that $Q_e^{(S)} = L_S R_e^{(S)} L_S^{-1}$ is the identity transformation on $\mathfrak{H}$. Also $\psi_{I,T}(e, k) = [\phi_{I,T}(e, kL_T)]L_T^{-1} = kL_T L_T^{-1} = k$, $\psi_{S,I}(e, k) = [\phi_{S,I}(eL_S, k)]L_S^{-1}$ $= [\phi_{S,I}(c_S, k)]L_S^{-1} = kL_S L_S^{-1} = k$ as desired.

8. **Direct products.** If the quasigroups $\mathfrak{H}_{S,T}$ in Theorem 7 are all equal

(6) This type of study has its inspiration in the theory of crossed extensions defining simple algebras as in my *Non-associative algebras. II. New simple algebras*, Ann. of Math. vol. 43 (1942) pp. 708–723. It originates, of course, in the theory of crossed products. Note that Bruck's construction of crossed extensions actually arose from an attempt to construct more general simple algebras and will be presented by him in this connection.

to $\mathfrak{H}$ the crossed extension $(\mathfrak{H}, \Lambda, \phi)$ satisfies the usual definition(7) of the direct product $\mathfrak{H}\times\Lambda$. It is a loop containing $\mathfrak{H}$ as a subloop. Its elements j_S form a loop isomorphic to Λ and it is customary to assume that every $j_S = S$ and that Λ is also a subloop of $\mathfrak{H}\times\Lambda$. We may now prove

THEOREM 7. *Let $\mathfrak{H}$ and $\mathfrak{A}$ be normal divisors of a loop $\mathfrak{G}$ such that the intersection of $\mathfrak{H}$ and $\mathfrak{A}$ is the identity element of $\mathfrak{G}$. Then $\mathfrak{H}\mathfrak{A} = \mathfrak{H}\times\mathfrak{A}$.*

For, by Theorem 7, $\mathfrak{H}\mathfrak{A}/\mathfrak{H} \cong \mathfrak{A}$ and $\mathfrak{H}\mathfrak{A}$ is the crossed extension $\mathfrak{L} = (\mathfrak{H}, \mathfrak{A}, \phi)$. Then $\mathfrak{L} = \mathfrak{H}\times\mathfrak{A}$ if and only if $(ah)(bk) = (ab)(hk)$ for every a and b of $\mathfrak{A}$, h and k of $\mathfrak{H}$. But $(ah)(bk) = (ab)\,h_0$ where h_0 is in the normal divisor $\mathfrak{H}$ of $\mathfrak{G}$. Since $\mathfrak{A}$ is also a normal divisor of $\mathfrak{G}$ and $(\mathfrak{A}h)(\mathfrak{A}k) = \mathfrak{A}hk$ we have $(ah)(bk) = a_0(hk)$ for a_0 in $\mathfrak{A}$. By the corollary to Theorem 2 we have $(ab)h_0 = a_0(hk)$ only if $a_0 = ab$, $(ah)(bk) = (ah)(hk)$ as desired(8).

9. **Automorphisms.** An automorphism S of any multiplicative system $\mathfrak{G}$ is a nonsingular transformation S on $\mathfrak{G}$ such that $(xS)(yS) = (xy)S$. Then $xSR_z = xR_yS$ where $z = yS$ and

$$R_{yS} = S^{-1}R_yS \tag{10}$$

for every y in $\mathfrak{G}$. Thus the set $\mathfrak{G}_r$ of all right multiplications of $\mathfrak{G}$ has the property that $S^{-1}TS$ is in $\mathfrak{G}_r$ for every T of $\mathfrak{G}_r$.

The transformation group $\mathfrak{G}_\rho$ generated by the right multiplications of $\mathfrak{G}$ is now carried into itself by the inner automorphisms

$$T \to S^{-1}TS$$

of the group of all nonsingular transformations on $\mathfrak{G}$. Thus every automorphism S of $\mathfrak{G}$ determines a unique automorphism

$$S_\rho: \qquad T \to TS_\rho = S^{-1}TS$$

of $\mathfrak{G}_\rho$. If $S_\rho = U_\rho$ then $S^{-1}R_xS = U^{-1}R_xU$ for every x and $R_{xS} = R_{xU}$. In the case where $\mathfrak{G}$ is either a quasigroup or a ring without absolute right divisors of zero this implies that $xS = xU$. Then $S = U$ and the correspondence $S \to S_\rho$ is one-to-one. It is evidently preserved under multiplication. We have a similar result for left multiplications and see also that each S determines an automorphism S_τ of $\mathfrak{G}_\tau$. Thus we have proved

THEOREM 8. *The group of all automorphisms of a quasigroup $\mathfrak{G}$ is isomorphic to a subgroup of the automorphism groups of each of its transformation groups $\mathfrak{G}_\rho$, $\mathfrak{G}_\lambda$, $\mathfrak{G}_\tau$.*

We shall not state the analogous results for algebras and for rings without

(7) Cf. R. H. Bruck, *Some results in the theory of quasigroups*, Trans. Amer. Math. Soc. vol. 55 (1944) pp. 19–52.

(8) This proof seems more direct and an improvement over the one usually given in the associative case.

absolute divisors of zero.

We may also prove

THEOREM 9. *Let $\mathfrak{G}$ be a loop with identity element e and S be a nonsingular transformation on $\mathfrak{G}$ such that $T\to S^{-1}TS$ is an automorphism S_τ of $\mathfrak{G}_r$. Then S is an automorphism of $\mathfrak{G}$ if and only if $eS=e$, $\mathfrak{G}_rS_\tau=\mathfrak{G}_r$.*

For if $\mathfrak{G}_rS_\tau=\mathfrak{G}_r$ then $R_xS_\tau=S^{-1}R_xS=R_z$, $yz=yS^{-1}R_xS=(yS^{-1})xS$. Put $y=e$ and use $eS=e$, $e=eS^{-1}$ to obtain $z=xS$, $(yS)z=(yS)(xS)=(yS)S^{-1}R_xS=(yx)S$. Thus S is an automorphism of $\mathfrak{G}$. The converse follows from (10) and the fact that an automorphism S of $\mathfrak{G}$ necessarily leaves its identity element unaltered.

We note that an antiautomorphism of a system $\mathfrak{G}$ is a nonsingular transformation J on $\mathfrak{G}$ such that $(xJ)(yJ)=(yx)J$, $JR_x=L_yJ$,

$$R_{yJ}=J^{-1}L_yJ, \qquad L_{xJ}=J^{-1}R_xJ. \tag{11}$$

Then the automorphism J_τ of $\mathfrak{G}_r$ defined by $T\to J^{-1}TJ$ carries $\mathfrak{G}_r$ into $\mathfrak{G}_l$, $\mathfrak{G}_l$ into $\mathfrak{G}_r$. Conversely if $eJ=e$ and $J^{-1}\mathfrak{G}_rJ=\mathfrak{G}_l$ we have $J^{-1}R_xJ=L_x$, $zy=yJ^{-1}R_xJ$, $eJ^{-1}=e$, $ze=z=xJ$, $(xJ)(yJ)=(yx)J$. We have proved

THEOREM 10. *Let $\mathfrak{G}$ be a loop with identity element e and J be a nonsingular transformation on $\mathfrak{G}$ such that $T\to J^{-1}TJ$ is an automorphism J_τ of $\mathfrak{G}_r$. Then J is an antiautomorphism of $\mathfrak{G}$ if and only if $eJ=e$, $\mathfrak{G}_rJ_\tau=\mathfrak{G}_l$.*

10. **Isotopes with a prescribed identity element.** Multiplication in a loop $\mathfrak{G}$ with identity element e is defined by

$$x\cdot eS = xS \tag{12}$$

for every right multiplication S of $\mathfrak{G}_r$. Let P and Q be any permutations of $\mathfrak{G}$ and define

$$\mathfrak{M} = P\mathfrak{G}_rQ, \tag{13}$$

so that the elements of $\mathfrak{M}$ are the permutations PSQ. Suppose also that f is any fixed element of $\mathfrak{G}$. We write.

$$(x, fT) = xT \tag{14}$$

for every $T=PSQ$ and prove

THEOREM 11. *The system $\mathfrak{G}^{(0)}$ defined by* (13), (14) *is a quasigroup isotopic to $\mathfrak{G}$ such that $\mathfrak{G}_r^{(0)}=\mathfrak{M}$,*

$$R_{fT}^{(0)} = T. \tag{15}$$

Then f is the identity element of $\mathfrak{G}^{(0)}$ if and only if the identity permutation is in $\mathfrak{M}$.

For $y=fT=fPR_aQ=(fP\cdot a)Q=aLQ$, where L is the left multiplication de-

fined by the element fP of $\mathfrak{G}$. Thus (14) is equivalent to

$$(x, y) = (xP \cdot yQ^{-1}L^{-1})Q, \tag{16}$$

and defines an isotope of $\mathfrak{G}$. Every y of $\mathfrak{G}^{(0)}$ has the form $y=fT$ for T in $\mathfrak{M}$ and (14) defines $R_y^{(0)}=T$. Then $\mathfrak{G}_r^{(0)}=\mathfrak{M}$. If the identity permutation I is in $\mathfrak{M}$ the value $T=I$ in (14) gives $(x, f)=x$ and $(f, y)=(f, fT)=fT=y$ implies that f is the identity element of $\mathfrak{G}^{(0)}$. Conversely if f is the identity element of $\mathfrak{G}^{(0)}$ we have $R_f^{(0)}=I$ in $\mathfrak{M}=\mathfrak{G}_r^{(0)}$ as desired.

Let us close this section with the introduction of two new fundamental concepts. We recall that in classifying associative algebraic systems it is customary to place two systems in different classes if and only if they are neither isomorphic nor anti-isomorphic. In studying nonassociative systems we replace isomorphism by isotopism and so should introduce the following concepts. Let $\mathfrak{G}$ and $\mathfrak{G}'$ be algebraic systems. Then we shall say that $\mathfrak{G}$ and $\mathfrak{G}'$ are *anti-isotopic* if there exist one-to-one mappings S, T, U on $\mathfrak{G}$ to $\mathfrak{G}'$ such that $xS \cdot yT=(y \cdot x)U$ for every x and y of $\mathfrak{G}$. Clearly $\mathfrak{G}$ *and* $\mathfrak{G}'$ *are anti-isotopic if and only if* $\mathfrak{G}$ *is isotopic to a system which is anti-isomorphic to* $\mathfrak{G}'$.

In a similar fashion we say that $\mathfrak{G}$ is *antihomotopic* to $\mathfrak{G}$ if there exist equivalent mappings S, T, U on $\mathfrak{G}$ to $\mathfrak{G}'=\mathfrak{G}S=\mathfrak{G}T=\mathfrak{G}U$ such that $xS \cdot yT=(y \cdot x)U$. Then $\mathfrak{G}$ *is antihomotopic to* $\mathfrak{G}'$ *if and only if* $\mathfrak{G}$ *is homotopic to a system anti-isomorphic to* $\mathfrak{G}$.

A program for the classification of loops may now be made as follows. We first classify loops into classes such that no two loops in the same class are isomorphic or anti-isomorphic. We then determine which classes are isotopic and will know that two systems in different sets of isotopic classes will be neither isotopic nor anti-isotopic.

11. **Finite quasigroups.** A finite quasigroup $\mathfrak{G}$ consists of a set of elements $e_1, e_2, \cdots, e_n$ and a corresponding set $\mathfrak{G}_r$ of permutations $R_1, R_2, \cdots, R_n$ on $\mathfrak{G}$ such that $x_iR_j=x_iR_k$ for any i if and only if $j=k$. We define multiplication in $\mathfrak{G}$ by $e_ie_j=e_iR_j$ and e_1 is the identity element of $\mathfrak{G}$ if and only if $e_1R_i=e_i$, R_1 is the identity permutation.

If $\mathfrak{H}$ is a subset of $\mathfrak{G}$ and x is in $\mathfrak{G}$ the set $x\mathfrak{H}$ consists of all xh for h in $\mathfrak{H}$. If $xh=xk$ then $h=k$ and the number of elements in $x\mathfrak{H}$ is the same as the number of elements in $\mathfrak{H}$. If $\mathfrak{H}$ is a subquasigroup of $\mathfrak{G}$ and $xh=k$ where h and k are in $\mathfrak{H}$ then x is in $\mathfrak{H}$. But then $x\mathfrak{H}$ and $\mathfrak{H}$ have an element in common if and only if $x\mathfrak{H}=\mathfrak{H}$.

Let m be the order of $\mathfrak{H}$ and $\mathfrak{H}$ be a proper subquasigroup of $\mathfrak{G}$. By the argument above $2m \leqq n$. It follows that the largest order of $\mathfrak{H}$ is the greatest integer in $n/2$. It is known(9) that there exist quasigroups of every order n with a subquasigroup of this maximum order.

If each element of $\mathfrak{G}$ is in one and only one subset $x\mathfrak{H}$ and the mapping

(9) Cf. Bruck, loc. cit.

$x \to x\mathfrak{H}$ is a homomorphism, the subquasigroup $\mathfrak{H}$ of $\mathfrak{G}$ is called[10] a normal divisor of $\mathfrak{G}$. Using this definition we may prove[11]

THEOREM 12. *Let $\mathfrak{H}$ be a subquasigroup of order m of a quasigroup $\mathfrak{G}$ of order $2m$. Then $\mathfrak{H}$ is a normal divisor of $\mathfrak{G}$.*

For let $\mathfrak{A}$ consist of all elements of $\mathfrak{G}$ not in $\mathfrak{H}$. If a is in $\mathfrak{A}$ the argument above implies that $a\mathfrak{H} \subset \mathfrak{A}$. But $\mathfrak{A}$ and $a\mathfrak{A}$ each consist of m elements, $a\mathfrak{H} = \mathfrak{A}$. Similarly $\mathfrak{H}a = \mathfrak{A}$. It follows that $\mathfrak{G}$ consists of the two distinct cosets $\mathfrak{H}$ and $\mathfrak{A}$. Now $\mathfrak{H}\mathfrak{H} = \mathfrak{H}$, $\mathfrak{A}\mathfrak{H} \supset a\mathfrak{H} = \mathfrak{A}$, every $a\mathfrak{H} \subset \mathfrak{A}$, $\mathfrak{A}\mathfrak{H} = \mathfrak{A}$. Similarly $\mathfrak{H}\mathfrak{A} = \mathfrak{A}$. If $a(ah)$ is not in $\mathfrak{H}$ then $a(ah) = ah_0$ for h_0 in $\mathfrak{H}$, $ah = h_0$ whereas we are assuming that a is in $\mathfrak{A}$. Thus $a\mathfrak{A} \subset \mathfrak{H}$, $a\mathfrak{A}$ consists of m elements, $a\mathfrak{A} = \mathfrak{H}$, $\mathfrak{A}\mathfrak{A} = \mathfrak{H}$. Clearly $x \to x\mathfrak{H}$ is a homomorphism of $\mathfrak{G}$ on the cyclic group $\mathfrak{G}/\mathfrak{H}$ of order two.

12. **Solvable loops.** A group of prime order has no nontrivial subgroups and it is this property which is critical in the theory of solvable groups[12]. A loop of prime order may have proper subloops other than the identity loop and so we shall make the

DEFINITION. *A loop $\mathfrak{G}$ is called* **solvable** *if none of its composition loops have nontrivial subloops.*

We then have

THEOREM 13. *Every subloop $\mathfrak{H}$ of a solvable loop $\mathfrak{G}$ is solvable and the composition loops of $\mathfrak{H}$ are isomorphic to a subset of those of $\mathfrak{G}$.*

The result is obvious if $\mathfrak{H}$ is a member of a composition series $\mathfrak{G}_0 \supset \mathfrak{G}_1 \supset \cdots \supset \mathfrak{G}_t \supset e$. Otherwise there is some $\mathfrak{G}_{i-1}$ such that $\mathfrak{G}_{i-1} \supset \mathfrak{H}$, $\mathfrak{G}_i$ does not contain $\mathfrak{H}$. By Theorem 2 the loop $\mathfrak{L} = \mathfrak{H}\mathfrak{G}_i$ has the property

$$\mathfrak{L}/\mathfrak{G}_i \cong \mathfrak{H}/\mathfrak{D}, \qquad \mathfrak{D} = \mathfrak{H} \cap \mathfrak{G}_i.$$

But $\mathfrak{H} \neq \mathfrak{D}$, $\mathfrak{L}/\mathfrak{G}_i$ is a subloop of $\mathfrak{G}_{i-1}/\mathfrak{G}_i$, $\mathfrak{L}/\mathfrak{G}_i$ has order greater than one, $\mathfrak{L}/\mathfrak{G}_i = \mathfrak{G}_{i-1}/\mathfrak{G}_i$, $\mathfrak{L} = \mathfrak{G}_{i-1}$. Then $\mathfrak{D}$ is a maximal normal divisor of $\mathfrak{H}$ contained in $\mathfrak{G}_i$. After a finite number of such steps we obtain a composition series $\mathfrak{H} = \mathfrak{D}_0 \supset \mathfrak{D}_1 \supset \cdots \supset \mathfrak{D}_s = [e]$ such that some $\mathfrak{D}_j = \mathfrak{G}_{i_j}$ or

$$\mathfrak{D}_{j-1}/\mathfrak{D}_j \cong \mathfrak{G}_{i_{j-1}}/\mathfrak{G}_{i_j}.$$

In either case the result of our theorem follows.

If $\mathfrak{H}$ is a normal divisor of a loop $\mathfrak{G}$ the homomorphism of $\mathfrak{G}$ to $\mathfrak{G}/\mathfrak{H}$ implies, exactly as for groups, that $\mathfrak{G}$ is solvable if and only if both $\mathfrak{H}$ and $\mathfrak{G}/\mathfrak{H}$ are solvable.

---

[10] This includes our definition of normal divisor for loops.

[11] This theorem and its proof were suggested to me by Daniel Zelinsky, a graduate student at the University of Chicago. See also G. N. Garrison, *Quasigroups*, Ann. of Math. vol. 41 (1940) pp. 474–487. The results of Garrison imply our theorem although it was not explicitly stated. Note also that Garrison proved a case of our Theorem 4 as his Theorem 4.24.

[12] We regard the associative case of Theorem 13 as the principal result of that theory.

13. **Right powers.** If x is the only element of a quasigroup $\mathfrak{G}$ we define the *right power* x^k inductively by $x^k = x^{k-1}x$ for every positive integer k. If $\mathfrak{G}$ is a loop with identity element e then the right order of $x \neq e$ is the least positive integer t such that $x^t = e$. Now $x = eS$ where $S = R_x$, $x^2 = xS = eS^2$, $\cdots$, $x^{k-1} = eS^{k-1}$, $x^k = (eS^{k-1})x = eS^k$. Hence t is the least positive integer such that the permutation R_x^t leaves e unaltered. The permutation R_x is in the group $\mathfrak{G}_\rho$ and hence $S^\alpha = I$ where α is the order of $\mathfrak{G}_\rho$. But the usual proof implies that t divides α. Since $e, eS, \cdots, eS^n$ cannot all be distinct the right order of x is at most n and we have

THEOREM 14. *The right order of an element of a finite loop $\mathfrak{G}$ of order n is at most n and is a divisor of the order of $\mathfrak{G}_\rho$.*

We may also prove

THEOREM 15. *Let S be a right multiplication of $\mathfrak{G}$ and t be the number of letters in a cycle of S. Then there exists a loop isotopic to $\mathfrak{G}$ and with an element having right order t.*

For if f is any element appearing in a cycle of S the letters of this cycle are $f, fS, \cdots, fS^{t-1}$. It follows that $fS^t = f$ and that $fS^k \neq f$ for $0 < k < t$. We use Theorem 11 to define an isotope of $\mathfrak{G}$ with f as identity element and $\mathfrak{M} = \mathfrak{G}_r$ such that $(x, fT) = xT$ for every right multiplication T of $\mathfrak{G}$. Then $a = fS$ has the property that its right power a^k, in the isotope, is equal to $(fS)^k = fS^k$ for every $k > 0$ and $a^k \neq f$ if $0 < k < t$, $a^t = fS^t = f$.

The construction above may be modified and we may take $\mathfrak{M} = P^{-1}\mathfrak{G}_r P$ in Theorem 11 where P is chosen so that $fP = e$. Then $a = eP^{-1}SP$ has right order t in an isotope with e as identity element.

14. **Quasigroups of order five.** The first step in the study of finite[13] loops $\mathfrak{G}$ of order n is the observation[14] that all loops of order $n \leqq 4$ are groups. Designate the elements of $\mathfrak{G}$ by $e_1, \cdots, e_n$ and R_{e_i} by R_i and assume henceforth that R_1 is the identity permutation. Then $R_2, \cdots, R_n$ are permutations on n letters and $R_i = (1, i, \cdots)$. Conversely if $(1, i, \cdots)$ is in $\mathfrak{G}_r$ then $(1, i, \cdots) = R_i$. Moreover if $R_2, \cdots, R_{n-1}$ are given, the permutation R_n is uniquely determined by the fact that $e_i R_n \neq e_i R_j$ for $j = 1, \cdots, n-1$.

We assume now that $n = 5$ and suppose first that $\mathfrak{G}_r$ contains a cycle on five letters. There is no loss of generality if we take this cycle to be (12345).

[13] Let $\mathfrak{G}$ be any finite loop and $R_1, \cdots, R_n$ be the corresponding right multiplications. Regard the elements of $\mathfrak{G}$ as being a basis of a linear space of order n over some field, and define a linear transformation S_i on this space as the correspondence in which each basal element e_j is replaced by $e_j R_i$. Define $S_i S_k = S_t$ where t is defined by $e_i R_k = e_t$. Then our set of linear transformations forms a loop with respect to this operation, and we have the geometry of the invariants under this loop to study. It would be interesting to discover whether there are more general transformation loops.

[14] This result was mentioned in the paper of Bruck referred to in footnote 7. It is easy to prove and seems to be fairly well known.

Assume also that R_3 is a cycle. The possible values of R_3 are then (13524), (13542), (13254). The values (13524), (14253), (15432) occur in the case where $\mathfrak{G}$ is the group.

Assume that $\mathfrak{G}$ is not a group and that $R_2=(12345)$, $R_3=(13524)$. If $e_4R_4=e_2$ then $e_2R_4\neq e_2, e_3, e_4$ so that $e_2R_4=e_1$ or e_5. In the former case $R_4=(142)(35)$ whereas $e_3R_3=e_5$. In the latter case $R_4=(14253)$ so that $R_5=(15432)$ contrary to our hypothesis that $\mathfrak{G}$ is not a group. Hence $e_4R_4\neq e_2, e_4, e_5, e_1$ so that $e_4R_4=e_3$. Now $R_4\neq(143)(25)$ since $e_5R_3=e_2$, and $R_4\neq(14325)$ since $e_5R_2=e_1$. It follows that (12345), (13524) are right multiplications of the cyclic group only.

Consider next the case where $R_2=(12345)$, $R_3=(13542)$. Then we have a loop with right multiplications

(17) (12345), (13542), (14)(253), (15243).

If $R_4\neq(14)(253)$ then $e_4R_4\neq e_5, e_2, e_1, e_4$ so that $e_4R_4=R_3$. But $e_5R_2=e_1$ and thus $R_4\neq(14325)$. Hence $R_4=(143)(25)$ and we have the loop given by

(18) (12345), (13542), (143)(25), (15324).

Our final case with $R_2=(12345)$ and R_2 a cycle is that given by $R_3=(13254)$. The solution given by $R_4=(142)(35)$, $R_5=(15243)$ is isomorphic to that given by (18) since we obtain this loop from (18) by replacing e_3 by e_2, e_5 by e_3, e_2 by e_5 and thus (12345) by (15243), (13542) by (12345), (15324) by (13254), (143)(25) by (142)(35). There is no value of e_2R_4 possible except e_1 if $e_4R_4=e_2$ so that otherwise $e_4R_4\neq e_4, e_2, e_5, e_1$, and $R_4=(14352)$, $R_5=(153)(24)$. Replace e_5 by e_2, e_2 by e_4, e_4 by e_5 in (18) and so replace (12345) by (14352), (13542) by (13254), (15324) by (12345) and (143)(25) by (153)(24). We have shown that all loops which are not groups and which have $R_2=(12345)$ and R_3 a cycle are isomorphic to (17) and (18). The latter two loops are neither isomorphic nor anti-isomorphic since the loop defined by (17) contains an element of order two and that defined by (18) does not.

Let us suppose that $R_2=(12345)$ and that R_3 is not a cycle. Then a solution is given by

(19) (12345), (13)(254), (14352), (15324).

With R_2 and R_3 as in (19) the hypothesis $R_4\neq(14352)$ implies that $R_4\neq(14325)$, $e_4R_4\neq e_3, e_4, e_2, e_5, e_4R_4=e_1$. Then $R_4=(14)(235)$ or (14)(253). Neither value is possible since $e_2R_2=e_3$, $e_2R_3=e_5$. Thus we must assume that $R_3\neq(13)(254)$. But $R_3\neq(13)(245)$. Hence $e_3R_3\neq e_1, e_3, e_4$. If $e_3R_3=e_2$ then $R_3\neq(132)(45)$, $e_3R_3\neq e_1$, R_3 is a cycle. The only possibility remaining is that where $e_3R_3=e_5$ and we see that $e_5R_3\neq e_1$ since $e_5R_2=e_1$. Then $e_5R_3=e_4$ or e_2 and in either case R_3 is a cycle, contrary to hypothesis.

The loop given by (19) is not isomorphic or anti-isomorphic to that given by (18) since the former contains an element of order two and the latter does

not. In (19) we have $x^2=e_3$ for $x=e_2, e_4, e_5$, $(x^2)^2=e_1$. Hence no two of the loops obtained thus far are either isomorphic or anti-isomorphic.

There remains only the case of loops $\mathfrak{G}$ such that $\mathfrak{G}_r$ contains no cycle. If $e_2R_2=e_1$ we may assume that $R_2=(12)(345)$. A solution is then given by

(20) (12)(345), (13)(254), (14)(235), (15)(243)

which defines a loop containing four subgroups of order two and which is neither isomorphic nor anti-isomorphic to any of the loops obtained above. If R_2 and R_3 are as in (20) the assumption of a different R_4 implies that $e_4R_4\neq e_4, e_5, e_2, e_1$ so that $e_4R_4=e_3$, $e_3R_4\neq e_1$, R_4 is a cycle; a contradiction. Hence let $R_3\neq(13)(254)$. From our value of R_2 we have $R_3\neq(13)(245)$ and we also know that $R_3\neq(13245), (13254)$. But $e_3R_3\neq e_1, e_4, e_3$. Hence $e_3R_3=e_2$ or e_5 and $R_3\neq(132)(45)$, so that $e_3R_3=e_5$. We thus obtain $R_3=(135)(24)$. It follows that $e_4R_4\neq e_4, e_5, e_2$ and that $e_4R_4=e_1, e_3$. The values (14)(235) and (14)(253) are impossible since $e_3R_3=e_5$, $e_5R_2=e_3$. Hence $e_4R_4=e_3$ and we have the loop defined by

(21) (12)(345), (135)(24), (143)(25), (154)(23).

This loop contains only one element of order two and no elements of right order five and is not isomorphic to any of the loops obtained above. Its left multiplications are readily computed and are (12)(345), (13524), (14325), (15423). Interchange e_2 and e_4 and we obtain (17). Thus the loop defined by (21) is anti-isomorphic to the loop defined by (17). We have proved

THEOREM 16. *Every loop of order five is either a group or is isomorphic to one of the loops defined by the sets* (17), (18), (19), (20), (21) *of right multiplications. No two of the latter loops are isomorphic or anti-isomorphic except that the loop defined by* (21) *is anti-isomorphic to that defined by* (17).

If we replace each permutation S of (20) by $P^{-1}SP$ where $P=(12)(345)$ we replace (12)(345) by itself, (13)(254) by (135)(24), (14)(235) by (143)(25), (15)(243) by (154)(23). By Theorem 11 the loops defined by (20) and (21) are isotopic. Replace the permutations R_1, R_2, R_3, R_4, R_5 of (20) by $R_4^{-1}=(14)(253)$, $R_2R_4^{-1}=(15243)$, $R_3R_4^{-1}=(12345)$, $R_4R_4^{-1}=I$, $R_5R_4^{-1}=(13542)$. By Theorem 11 the loop defined by (17) is isotopic to that defined by (20). Replace each permutation S of (18) by $P^{-1}SP$ where $P=(13542)$. This replaces (12345) by (15243), (13542) by itself, (143)(25) by (14)(253) and (15324) by (12345). Hence (18) is isotopic to (17) and thus also to (20). We finally replace the permutations R_i of (19) by $R_1R_3^{-1}=(13)(245)$, $R_2R_3^{-1}=(142)(35)$, $R_3R_3^{-1}$, $R_4R_3^{-1}=(154)(23)$, $R_5R_3^{-1}=(125)(34)$. Interchange e_2 and e_3 and obtain (21). Thus (19) is isotopic to (21) and hence to (20). We have proved that all quasigroups of order five are isotopic either to a group or to the loop defined by (20). We state our result as the following

THEOREM 17. *All quasigroups of order five not isotopic to the group are isotopic to each other.*

15. **Loops of order six.** While a complete study of loops of order six would probably yield some interesting and suggestive results we shall not carry it out here but shall rather content ourselves with a list of some special types of loops.

The first of our examples is that given by the right multiplications

(22) (123456), (135)(246), (143652), (153264), (163)(254).

This loop contains no subloops of order two since it contains no elements of right order two. Its elements of right order three are e_3 and e_6, and $e_6^2 = e_3$. Thus a subloop of order three would contain e_3 as well as $e_3^2 = e_6$, e_1, $e_3e_6 = e_2$, a contradiction. It follows that our loop has no nontrivial subloops and is simple([15]).

A simple loop containing elements of right order four is given by

(23) (123456), (1364)(25), (146532), (1543)(26), (1635)(24).

It clearly contains no nontrivial subloops. It is isotopic to the loop defined by replacing each right multiplication S by $P^{-1}SP$ where $P = (654321)$. This latter simple loop contains three subloops of order two and is given by

(24) (123456), (13)(2465), (14)(2536), (15)(2643), (163542).

Let us now consider loops $\mathfrak{G}$ of order six with a subloop $\mathfrak{H}$ of order three. All *groups* of order six are of this kind. Then $\mathfrak{H}$ is a normal divisor of $\mathfrak{G}$, $\mathfrak{G}$ is the crossed extension $(\mathfrak{H}, \Lambda, \phi)$. Also $\mathfrak{H}$ is the cyclic group $e = e_1$, $f = e_2$, $f^2 = e_3$ such that $f^3 = e$, Λ is the group (I, S) of order two, $\mathfrak{H}_{S,I} = \mathfrak{H}$. Then the elements of $\mathfrak{G}$ are

$$e, f, f^2, g, gf, gf^2$$

such that $(gf^i)f^j = g(f^{i+j})$ for every $i, j = 0, 1, 2$. It follows that the first three right multiplications of all such loops are given by the identity,

(25) (123)(456), (132)(465).

Since $\mathfrak{H}_{I,S}$ has e as a left identity element we either have $\mathfrak{H}_{I,S} = \mathfrak{H}$ and

(26) $$f^i(gf^j) = gf^{i+j} \qquad (i, j = 0, 1, 2),$$

([15]) In a letter to Bruck I conjectured the theorem stating there exist simple loops of all orders n except 4. Bruck has proved this result and the proof will appear elsewhere. It was suggested to me by the example of order six which I constructed as showing that the Sylow theory does not hold for loops. Observe also that our two loops of order six are solvable. However they are isotopic to loops which have proper subloops and which are therefore not solvable (this observation is due to Bruck).

or the left multiplications in $\mathfrak{H}_{I,S}$ are the identity, $L_f=(132)$, $L_{f^2}=(123)$ and the resulting relations are

$$f^i(gf^j) = gf^{2i+j} \qquad (i, j = 0, 1, 2). \tag{27}$$

Thus these portions of the multiplication table of a loop $\mathfrak{G}$ of order six are exactly the same as when $\mathfrak{G}$ is a group.

The right multiplications of the quasigroup $\mathfrak{H}_{S,S}$ are either the cycle (123) and its powers or the permutations (12), (23), (31). There are six possible arrangements of each set of three multiplications and hence twelve values of $\phi_{S,S}$. The relations

$$(gf^i)(gf^j) = f^{\alpha+\beta i+\gamma j} \qquad (i, j = 0, 1, 2) \tag{28}$$

for $\alpha=0$, 1, 2, for $\beta=1$, 2, and for $\gamma=1$, 2 give twelve distinct values for $\phi_{S,S}$ and so all possible values. Write $f^2=d$ and obtain $f^{2i}=d^i$, $(f^{2i})(gf^{2j})=gf^{2(i+j)}=d^i(gd^j)=gd^{i+j}$ in (26), $(f^{2i})(gf^{2j})=gf^{4i+2j}=(d^i)(gd^j)=gd^{2i+j}$ in (27). However $(gf^{2i})(gf^{2j})=f^{\alpha+2\beta i+2\gamma j}=(gd^i)(gd^j)=d^{2\alpha+\beta i+\gamma j}$. It follows that we may delete the value $\alpha=2$ in our classification of loops and so reduce the number of cases of (20) to eight.

If $\beta=\gamma$ the value $\alpha=0$ implies that $g^2=e$, $(gf)^2=f^{2\beta}$, $(gf^2)^2=f^{4\beta}=f^{\beta}$ so that we may always choose an element g such that $\alpha=1$. When (26) holds and $\beta=\gamma=1$ we have the cyclic group. When (26) holds and $\beta=\gamma=2$ the resulting loop is the only other commutative loop in our set. Its right multiplications are given by (25) and

$$(14)(2536),\ (1526)(34),\ (1635)(24). \tag{29}$$

These loops are evidently self-anti-isomorphic. When (27) holds and $\alpha=1$ then $\beta=\gamma=1$ yields

$$(1426)(35),\ (15)(2436),\ (1634)(25), \tag{30}$$

and $\beta=\gamma=2$ yields

$$(142635),\ (153624),\ (16)(25)(34). \tag{31}$$

Evidently no one of our four loops is isomorphic to any of the other three.

If (27) holds the mapping $f\to f$, $g\to g$, $fg\to gf$ induces an anti-isomorphism of $\mathfrak{G}$ on a loop of the same elements such that all elements are invariant except that gf and gf^2 are interchanged. Then $(f^ig)(f^jg)=(gf^{2i})(gf^{2j})\to(gf^i)(gf^j)$. But $(gf^{2i})(gf^{2j})=f^{\alpha+2\beta j+2\gamma i}$ so that the result of replacing γ by 2β and β by 2γ in (28) is a loop anti-isomorphic to the original. Thus (30) and (31) are anti-isomorphic.

When (26) holds the loops defined by (28) for $\beta=1$, $\gamma=2$ are anti-isomorphic to those defined for $\beta=2$, $\gamma=1$. If $\gamma=2\beta=2$ then $\alpha=0$ yields

$$(14)(25)(36),\ (15)(26)(34),\ (16)(24)(35), \tag{32}$$

while $\alpha=1$ yields

(33) (142536), (152634), (162435).

Their anti-isomorphs determined by $\beta=2\gamma=2$ are given, respectively, by

(34) (14)(2536), (15)(2634), (16)(2435),

and

(35) (1425)(36), (1526)(34), (1624)(35).

When (27) holds and $\beta\neq\gamma$ the loops defined are self-anti-isomorphic. The value $\alpha=0$ defines the noncommutative group of order six if $\beta=1$ and $\gamma=2$, and yields the loop defined by

(36) (14)(2635), (15)(2436), (16)(2534)

for $\beta=2$, $\gamma=1$. The set of values $\alpha=1$, $\gamma=2\beta=2$ defines

(37) (1426)(35), (1524)(36), (1625)(34),

and $\alpha=1$, $\beta=2\gamma=2$ defines

(38) (142635), (152436), (162534).

Every loop $\mathfrak{G}$ of order six with a subloop $\mathfrak{H}$ of order three has now been shown to have a single subloop of that order. The property (26) states that for such loops the centralizer of $\mathfrak{H}$ is $\mathfrak{G}$, and (27) states that for those loops it is $\mathfrak{H}$. Hence no one of the loops defined by (29), (32), (33), (34), (35) is isomorphic to any one of the loops defined by (30), (31), (36), (37), (38) or to either of the two groups of order six. Clearly no one of our twelve loops is isomorphic to any one of the remaining eleven. The two groups and the loops defined by (29), (36), (37), (38) are self-anti-isomorphic, and the loops defined by (31), (34), (35) are the anti-isomorphs, respectively, of the loops defined by (30), (32), (33).

The general theory implies that all isotopes of a loop with a normal divisor of order m contain a normal divisor of order m. Moreover we may obtain isomorphs of all loops isotopic to a loop $\mathfrak{G}$ if we use as right multiplications the products $SR_1, SR_2, \cdots, SR_n$ where $R_1, \cdots, R_n$ are the right multiplications of $\mathfrak{G}$, S^{-1} is any one of the R_i.

By direct computation we see that if $A=(123)(456)$ and $B=(14)(2536)$ then $AB=(1526)(34)$, $A^2B=(1635)(24)$. It follows that the right multiplications of the loop defined by (29) are I, A, A^2, B, AB, A^2B. Then $A^{-1}=A^2$, $S=I$, A, A^2 give isomorphic loops. If we take $S=B^{-1}=(14)(2635)$ we obtain $B^{-1}A=(1536)(24)$, $B^{-1}A^2=(1625)(34)$, $B^{-1}B=I$, $B^{-1}AB=(456)(132)$, $B^{-1}A^2B=(B^{-1}AB)^2$. Interchange e_2 and e_3 and obtain the original right multiplications. The value $S=(AB)^{-1}$ gives S, $SA=B^{-1}A^{-1}A=B^{-1}$, $SA^2=B^{-1}A$, $SB=B^{-1}A^2B$, $SAB=I$, $SA^2B=B^{-1}AB$, and the value $S=(A^2B)^{-1}$ gives

$B^{-1}A^{-2}=B^{-1}A$, $B^{-1}A^2$, B^{-1}, $B^{-1}AB$, $B^{-1}A^2B$, I. Hence all loops isotopic to (29) are isomorphic to (29). Indeed we have proved that a loop is isotopic to a commutative loop $\mathfrak{G}$ of order six with a subloop of order three if and only if it is isomorphic to $\mathfrak{G}$.

Let $C=(1426)(35)$ in (30) and $A=(123)(456)$. Then $CA=(15)(2436)$, $CA^2=(1634)(25)$. Take $S=A^{-1}=A^2$ and replace our right multiplications by A^2, I, A, $A^{-1}C$, $A^{-1}CA$, $A^{-1}CA^2$. The loop so obtained and with right multiplications R_x is isomorphic to a loop whose right multiplications $R_x^{(0)}=AR_{xA}A^{-1}$ are A^2, I, A, CA, CA^2, C and is thus isomorphic to the original loop. Similarly if $S=A^{-2}=A$ then A, A^2, I, AC, ACA, ACA^2 may be replaced by A, A^2, I, $A^{-1}(AC)A=CA$, $A^{-1}(ACA)A=CA^2$, $A^{-1}(ACA^2)A=C$. The value $S=C^{-1}$ yields C^{-1}, $C^{-1}A$, $C^{-1}A^2$, I, A, A^2 where $C^{-1}=(1624)(35)$, $C^{-1}A=(1425)(36)$, $C^{-1}A^2=(1526)(34)$. Hence the loop defined by (30) is isotopic to that defined by (35). The value $S=(CA)^{-1}=(15)(2634)$ yields $(CA)^{-1}A=(16)(2435)$, $(CA^{-1})A^2=(14)(2536)$, $(CA)^{-1}CA$, $(CA)^{-1}(CA^2)=A$, $(CA)^{-1}C=A^{-1}=A^2$. Hence the loop defined by (30) is isotopic to that defined by (34). Finally $S=(CA^2)^{-1}$ yields $(CA^2)^{-1}=(1436)(25)$, $(CA^2)^{-1}A=(1534)(26)$, $(CA^2)^{-1}A^2=A^{-2}C^{-1}A^2=(3516)(24)=(1635)(24)$, $(CA^2)^{-1}C=A^{-2}=A$, $(CA^2)^{-1}(CA)=A^2$, I. Interchange e_2 with e_3, e_4 with e_5 and replace A by A^2, A^2 by A and our remaining right multiplications by those of (35).

Since (31) is anti-isomorphic to (30) and (32), (33) are anti-isomorphs of (33), (34) we see that (31) is isotopic to (32) and (33). Hence (30), (33), (34) are anti-isotopic, but not isotopic to (31), (32), (33).

We finally study (37) and see that if $B=(1426)(35)$ and $A=(123)(456)$ then $AB=(1625)(34)$, $A^2B=(1524)(36)$. Thus the values $S=A^{-1}$ and $S=A^{-2}$ replace our set of right multiplications by itself. If $S=B^{-1}$ then our multiplications are $B^{-1}=(1624)(35)$, $B^{-1}A=(A^{-1}B)^{-1}=(A^2B)^{-1}=(1425)(36)$, $B^{-1}A^2=(AB)^{-1}=(1526)(34)$, $B^{-1}AB=(465)(231)$, $B^{-1}A^2B=(456)(213)$. Interchange e_5 and e_6 to obtain (37). Next $S=(AB)^{-1}=(1526)(34)$, $(AB)^{-1}A=B^{-1}(AB^{-1})A^2=B^{-1}A$, $(AB)^{-1}AB=I$, $(AB^{-1})A^2B=B^{-1}AB$, $(AB^{-1})B=B^{-1}A^2B$. Finally $S=(A^2B)^{-1}=B^{-1}A$ gives the right multiplications $B^{-1}A$, $B^{-1}A^2$, B^{-1}, $B^{-1}AB$, $B^{-1}A^2B$, $B^{-1}AA^2B=I$. Interchange e_1 and e_3, e_5 and e_6 in (37) to obtain (36). We have proved that *every loop isotopic to* (36) *is isomorphic to* (36) *or* (37). Since (38) has not appeared in our determination of isotopes every loop isotopic to (38) is isomorphic to (38).

We have thus shown that there are six classes of loops of order six with a subloop of order three such that every loop of this kind is isotopic or anti-isotopic to a loop in one and only one class. The classes are: (1) *the isomorphs of the cyclic group*; (2) *the isomorphs of the noncommutative group*; (3) *the isomorphs of the commutative loop defined by* (29); (4) *the isomorphs of* (36); (5) *the isomorphs of* (37); (6) *the isomorphs and anti-isomorphs of* (30).

THE UNIVERSITY OF CHICAGO,
CHICAGO, ILL.