SOME RESULTS IN THE THEORY OF QUASIGROUPS

BY

RICHARD H. BRUCK

Introduction. The concept of *isotopy*, recently introduced(1) by A. A. Albert in connection with the theory of linear non-associative algebras, appears to have its value in the theory of *quasigroups*. Conversely, the author has been able to use quasigroups(2) in the study of linear non-associative algebras. The present paper is primarily intended as an illustration of the usefulness of isotopy in quasigroup-theory and as groundwork for a later paper on algebras, but is bounded by neither of these aspects.

The first two sections are devoted to the basic definitions of quasigroup and isotopy, along with some elementary remarks and two fundamental theorems due to Albert. Then there is initiated a study of special types of quasigroup, beginning with *quasigroups with the inverse property* (I. P. quasigroups). A system Q of elements $a, b, \cdots$ is called an I. P. quasigroup if it possesses a single-valued binary operation ab and there exist two one-to-one reversible mappings L and R of Q on itself such that

$$a^L(ab) = (ba)a^R = b \tag{1}$$

for every pair of elements a, b of Q.

Sections 3 to 9 inclusive are devoted in the main to I. P. quasigroups; in particular, to methods of constructing them and to their isotopy properties. In §3 will be found some elementary consequences of the definition (Lemma 1) and a construction of all I. P. quasigroups which are isotopic to a group (Theorem 3).

Lemma 2 (§4) gives necessary and sufficient conditions in order that an I. P. quasigroup may be constructed from a non-associative ring by use of the multiplication

$$xoy = x + y + xy. \tag{2}$$

In §5 the same matter is pursued further (in the special case that a cer-

Presented to the Society, November 27, 1943; received by the editors August 14, 1943.

(1) References to the bibliography are omitted from the Introduction, but will be found at appropriate places in the text.

(2) For example, let Q be a quasigroup of finite order $n \geqq 3$. Let F be a field containing at least 3 elements. To every element p of Q let there correspond an entity u_p, and let the entities u_p form a basis, in the usual sense, of a linear non-associative algebra A of order n over F. Let multiplication in A be given by $u_p \cdot u_q = h_{p,q} \cdot u_{pq}$, where the n^2 quantities $h_{p,q}$ are nonzero elements of F. (Such an algebra we call a *quasigroup-algebra*.) Then if Q is an I. P. quasigroup with a unique unit element, the $h_{p,q}$ can always be chosen so that A is both right-simple and left-simple (has no proper right or left ideals).

tain mapping J of the ring is linear) and leads to a specific construction. As a result we find (Theorem 4) that *for every odd prime p and for every integer n not less than 7 there exists an I. P. quasigroup Q of order p^n, which may be regarded as a (non-associative, noncommutative) extension of an abelian group of order p^{n-3} by another abelian group of order p^3.* Moreover Q is a *Moufang* quasigroup. (This last statement we shall explain in a later paragraph.) After demonstrating that a theory of coset expansions is impossible for general I. P. quasigroups, we show in §6 that for those I. P. quasigroups which are defined as above we may define normal sub-quasigroups in terms of invariant subrings and obtain the usual desirable features of cosets and quotient quasigroups (Theorem 5). Theorem 6, which was suggested by ideas of coset expansion but is otherwise unconnected with the rest of §6, gives an explicit construction of an I. P. quasigroup of index 2 over any I. P. quasigroup with a unique unit element. As a corollary we derive the existence of non-associative *I. P. quasigroups of order 2^n for every integer n not less than* 4.

Section 7 introduces three new types of quasigroup: *idempotent* quasigroups (those in which every element is idempotent), *unipotent* quasigroups (quasigroups with unique unit elements in which the square of every element is the unit element), and *totally symmetric* or T. S. quasigroups (in which a valid equation $ab=c$ remains true under every permutation of the letters a, b, c). Quasigroups of the first two types possess the inverse property if and only if they are totally symmetric. The main feature of this section is a construction by which there may be obtained from an idempotent quasigroup of order n a unipotent quasigroup of order $n+1$ and conversely. The construction preserves the inverse property. It is also shown that *there exist idempotent (unipotent) quasigroups of every finite order except order two (order three).* In §8 the above-mentioned construction is combined with the direct product to obtain a variety of T. S. quasigroups; these of course have the inverse property. In the same section necessary and sufficient conditions are given in order that an I. P. quasigroup with a unique unit element should possess an isotope which is totally symmetric (Theorem 7). It follows that *unipotent T. S. quasigroups are isotopic if and only if they are isomorphic* (Corollary 3). (The interest of this last result rests in the fact that it is an analogue of a theorem of Albert on groups (Theorem 2).) Theorem 8 gives necessary and sufficient conditions that an idempotent T. S. quasigroup should possess an I. P. isotope with a unit element, and a corollary exhibits an idempotent T. S. quasigroup of order 2^n-1 (for every integer n not less than 3) which does not possess an I. P. isotope with a unit element.

In §9 further attention is given to the special I. P. quasigroups, mentioned above, which D. C. Murdoch has called Moufang quasigroups after their originator, Miss R. Moufang. A *Moufang* quasigroup is a quasigroup with a unique unit element in which the elements obey the mild associative law

$$a(b\cdot cb) = (ab\cdot c)b. \tag{3}$$

The main result of the section (Theorem 9) is to the following effect. *A necessary and sufficient condition that every isotope, which possesses a unique unit element, of a quasigroup Q with a unit element should have the inverse property is that Q be a Moufang quasigroup.* In particular, an isotope of a Moufang quasigroup is a Moufang quasigroup provided it has a unit element. A similar result (Theorem 10) holds for alternative fields. The section also contains a brief sketch of the previously known theory of Moufang quasigroups.

Section 10 is devoted to the so-called *abelian* quasigroups of D. C. Murdoch. First it is shown that *every abelian quasigroup is isotopic to an abelian group, unique in the sense of isomorphism* (Theorem 11). This result is essentially Murdoch's. Next, an explicit construction is given of every isotope of an abelian group which is an abelian quasigroup in the sense of Murdoch (Theorem 12).

Section 11, which was prompted by an erroneous remark in a paper of Murdoch's, contains necessary and sufficient conditions that the *direct product* of two finite quasigroups should possess no sub-quasigroup except itself. The statement of these conditions (Theorem 13) is given in terms of the *invariant complexes* of G. N. Garrison.

In conclusion, the author would like to acknowledge his indebtedness to Professor Murdoch, from whom he has received a number of stimulating letters on quasigroups. The only item of conscious plagiarism, however, is a proof that every Moufang quasigroup has the inverse property. This appears as part of the proof of Theorem 9, and was copied directly from one of the letters.

1. **Quasigroups.** A *quasigroup Q* may be defined briefly as a multiplicative system such that if any two of the three letters a, b, c in the equation $ab=c$ be given as elements of Q the third is uniquely determined as an element of Q. This definition is equivalent to the following two laws:

I. *To every ordered pair a, b of elements of Q, whether distinct or not, there corresponds a unique element ab of Q, called the product of a and b.*

II. *For every pair a, b of elements of Q the equations $ax=b$ and $ya=b$ are uniquely solvable in Q for x and y.*

If in addition to I and II we assume the associative law $ab\cdot c=a\cdot bc$, the resulting system forms a group. Hence it is true in a sense that a quasigroup is a group minus the associative law, a group being a special type of quasigroup. However, various possibilities may occur in quasigroups which are impossible in groups, and it seems desirable to list a few of these.

(i) The unique solutions r, s of the equations $ar=a$, $sa=a$ may be distinct, and, moreover, may not be independent of a.

(ii) In general there may exist no element c, independent of b, such that $ax=b$ has the solution $x=cb$.

(iii) A quasigroup may contain more than one idempotent element $e(ee=e)$, or even none at all.

(iv) The order of a sub-quasigroup need not divide the order of the quasigroup.

(v) A quasigroup of prime order may possess proper sub-quasigroups, and a quasigroup of composite order may contain no sub-quasigroup except itself.

(vi) The *direct product* $P \times Q$ of two quasigroups P and Q, defined as the set of all couples (p, q) with p in P, q in Q under the multiplication

$$(p, q) \cdot (p', q') = (pp', qq'),$$

may not contain sub-quasigroups isomorphic to P or Q, or any proper sub-quasigroups whatsoever.

All of the above statements are well known, and, moreover, each will be justified (not necessarily with explicit comment) in the course of the present work. If the reader will keep them in mind, as hypothetical possibilities at least, it will lend point to the paper.

2. **Isotopy of multiplicative systems.** Although we shall use the notion of isotopy only in connection with quasigroups, we take the present opportunity to give it a more general setting. Let S be a system of elements $a, b, \cdots$, together with a binary operation $(\cdot)$, which associates with every ordered pair a, b a product $a \cdot b$ consisting of one or more elements of S. If $a \to a^U$ is any mapping of S into a subset of itself, and R is a subset of S, designate by R^U the set of elements a^U with $a \subset R$. Finally, let S_o be another system consisting of the same elements as S along with a binary operation (o). Then we say that S_o is *isotopic* to S if there exist three one-to-one reversible mappings U, V, W (not necessarily distinct) of S into itself, such that

$$aob = (a^U \cdot b^V)^W \tag{4}$$

for every pair of elements a, b of S. It is clear that isotopy is an equivalence relation. Two systems S, S_o may be related isotopically in more than one way; in particular, they are isomorphic (in the usual sense) if and only if it is possible to choose $U = P$, $V = P$, $W = P^{-1}$ for some one-to-one reversible mapping P of S into itself. It should be noted that *every isotope of a quasigroup is a quasigroup.*

To every fixed element b of a quasigroup Q there correspond two one-to-one reversible mappings of Q into itself, namely a right-mapping $R_b(a \to a \cdot b)$ and a left-mapping $L_b(a \to b \cdot a)$. As a matter of convenience we state two theorems on quasigroups which are entirely analogous to theorems(3) of A. A. Albert on linear algebras [1, Theorems 7, 18, pp. 698, 704, Theorem 12,

(3) Professor Albert [1, p. 696] defines two algebras A and A_o, which consist of the same elements, to be isotopic if there exist three nonsingular linear transformations P, Q, C of A such that $R_y^o = PR_zC$, $z = y^Q$, where R is the right-mapping $x \to x \cdot z$ and R_y^o is the corresponding mapping $x \to xoy$. Clearly this definition implies $xoy = (x^P \cdot y^Q)^C$, and conversely. The latter form was apparently first given by the present author (Bull. Amer. Math. Soc. abstract 48-1-8 (1942)).

p. 700](4). Since these theorems also appear in a paper by A. A. Albert in a recent issue of these Transactions, their proofs(5) will be omitted.

THEOREM 1. *Every quasigroup Q is isotopic to a quasigroup Q_0 with a unique two-sided unit element. If the relation between Q and Q_0 is given by* (4), *then*

$$U = PR_g^{-1}, \qquad V = PL_f^{-1}, \qquad W = P^{-1}, \tag{5}$$

where f, g are fixed elements of Q, and P is a permutation of the elements of Q (a one-to-one reversible mapping of Q upon itself). Moreover the unit element of Q_0 is u where $u^P = f \cdot g$.

THEOREM 2. *If Q_0 is a quasigroup with a unit element, isotopic to a group G, then Q_0 is in fact a group isomorphic to G.*

COROLLARY. *A non-associative quasigroup with a unit element is not isotopic to a group.*

So far as the author is aware, the concept of isotopy of systems with a binary operation had not been formulated in print(6) prior to the appearance of the papers of A. A. Albert [1]. It may be of interest to note, however, that a germ of this idea is now clearly visible in the (earlier) literature of quasigroups [2, 3, 4].

An intimate view of the workings of isotopy will be afforded by a consideration of the following quasigroup of order four:

(6)

·	1	2	3	4
1	3	1	4	2
2	4	2	1	3
3	1	3	2	4
4	2	4	3	1

Here the four elements 1, 2, 3, 4 of the quasigroup are arranged in the usual fashion, both as entries, in the form of a Cayley square, and as arguments, in the form of two borders which we may call the sideline and the headline. The ordered product $3 \cdot 4$, for example, is seen to be 4. Evidently we may form a (possibly) new quasigroup by subjecting the sideline, headline, or Cayley square to an arbitrary permutation of 1, 2, 3, 4. More generally, if Q and Q_0 are quasigroups of finite order, isotopically related by (4), and if the multi-

(4) Numbers in brackets designate references to the literature which may be found at the end of the paper.

(5) In the original form of the paper these proofs were given in detail. However they were essentially identical with those of Albert's paper [13], of which the author had been unaware.

(6) In a letter to D. C. Murdoch, dated October 17, 1939, H. Campaigne described essentially the same concept under a different name. The author has also seen an unpublished paper of S. Ulam in which an equivalent notion is considered.

plication table of Q is formed in the manner just described, the table for Q_θ may be obtained from that of Q by subjecting the sideline, headline, and Cayley square to the permutations U^{-1}, V^{-1} and W respectively. In classifying quasigroups according to isotopy it is sufficient, by virtue of Theorem 1, to consider only those with a unit element. As a more or less trivial consequence we may verify that every quasigroup with four elements or less is isotopic to a group, the quasigroup (6) being isotopic to the cyclic group of order 4.

In the case of quasigroups there is room for a slight broadening of the concept of isotopy (although we shall not alter the present definition) by admitting to the equivalence class of Q five other quasigroups formed essentially by permutation of the letters a, b, c in the relation $a \cdot b = c$. For example we obtain a quasigroup $Q(\times)$, in general not isotopic to Q, by defining $a \times c = b$ provided $a \cdot b = c$.

3. **Quasigroups with the inverse property.** Let there exist two one-to-one reversible mappings L, R of a quasigroup Q on itself such that

$$a^L(ab) = (ba)a^R = b \tag{7}$$

for all a, b of Q. In this case we shall speak of Q as a *quasigroup with the inverse property* (or as an I. P. quasigroup).

We note that the equations $ax = b$, $ya = b$ have the solutions $x = a^L b$, $y = ba^R$, respectively; a^L and a^R perform to this extent the duties of the inverse in a group, and may be spoken of as the *left-inverse* and *right-inverse* respectively of a in Q. As may readily be verified, the quasigroup (6) does not possess the inverse property. The best known I. P. quasigroups other than groups are those characterized by the mild associative law

$$a(b \cdot cb) = (ab \cdot c)b \tag{8}$$

and the existence of a unique two-sided unit element. Finite quasigroups of this type were introduced by R. Moufang [5], by whose name we shall refer to them from this point on, and were later studied by G. Bol [6].

We shall now derive some simple consequences of (7).

LEMMA 1. *If Q is any I. P. quasigroup, so that* (7) *holds, then*

(i) $L^2 = R^2 = I$, *the identity mapping*;

(ii) $(ab)^L = b^R a^R$, *and* $(ab)^R = b^L a^L$;

(iii) *if Q is commutative, $L = R$*;

(iv) *if Q has a unique two-sided unit element, $L = R$*;

(v) *if $L = R = J$, J is an anti-automorphism of Q*;

(vi) *if S and T are automorphisms of Q, of orders two or less (so that $S^2 = T^2 = I$), it follows that the quasigroup Q_θ defined by*

$$aob = a^S \cdot b^T \tag{9}$$

also has the inverse property. The mappings in Q_θ which correspond to L and R

in Q are

$$L_0 = STLS, \qquad R_0 = TSRT. \tag{10}$$

The last statement of Lemma 1 deserves some comment, since it gives a method of constructing I. P. quasigroups which are not groups. Evidently we could let Q be the symmetric group of order six, for example, since that group has an involutary automorphism, and could either take S and T equal or let one of them be the identity. As another more important example, we note from (iii) and (v) that we could let Q be any abelian group, since J would be available as an automorphism.

Proof of Lemma 1.

(i) By (7), $a^L(ab)=b$. Let $c=(a^L)^L$. Then, by (7), $cb=c[a^L(ab)]=ab$; whence $c=a$, since division is unique in a quasigroup. We have shown that $L^2=I$. Similarly, $R^2=I$.

(ii) Let $ab=c$ and use (7). We find, successively, $cb^R=a$, $c^La=b^R$, $b^Ra^R=c^L$, which is to say $(ab)^L=b^Ra^R$. The other identity is of course proved similarly.

(iii) By (7) and the commutative law, $(ab)a^L=(ab)a^R$, whence $a^L=a^R$, $L=R$.

(iv) Let u be the two-sided unit element of Q. By (7), $a^L(au)=u$, so $a^La=u$. Replacing a by a^L in the last relation, and using (i), we derive $aa^L=u$. Thus a^L, and similarly a^R, is a two-sided inverse of a. It follows that $L=R$.

(v) This follows from (ii).

(vi) Using (9), (10) and the hypotheses concerning S and T, we may verify by direct substitution that

$$b^{L_0}o(boa) = (avb)ob^{R_0} = a.$$

Since Q_0 is a quasigroup it is clear that L_0 and R_0 are unique.

We now study more closely the problem of constructing I. P. quasigroups which are isotopic to a given group.

THEOREM 3. *Let Q_0 be an I. P. quasigroup isotopic to a group $Q\equiv G$ via the equation*

$$aob = a^U \cdot b^V. \tag{11}$$

Then there exist a fixed element f of G and two automorphisms S, T of G, of orders one or two, such that (11) *may be replaced by*

$$aob = a^S \cdot f \cdot b^T. \tag{11.1}$$

Conversely (11.1) *defines an I. P. quasigroup for every f of G and for every pair S, T of involutary automorphisms of G.*

Since (11) is merely (4) with $W=I$, that is to say, Q_0 is a *principal isotope* of G[1, p. 698], it should be realized that (11.1) determines all I. P. quasi-

groups isotopic to G, to within an isomorphism.

Proof. The proof of the final statement of the theorem involves a straightforward calculation which we shall omit. Let u be the unit element of G, let a^J denote the inverse of a in G, and let R, L (we have dropped the subscript o) be the mappings which give the two inverses of a in Q_o. From (11), because of the hypothesis that Q_o has the inverse property, there results

$$b^{LU}\cdot(b^U\cdot a^V)^V = a, \qquad (a^U\cdot b^V)^U\cdot b^{RV} = a. \tag{12}$$

We recall that the mappings L_c, R_c of G are defined by $a\to ca$, $a\to ac$ respectively, and set

$$g = u^U, \qquad h = u^V, \qquad f = gh. \tag{13}$$

When $a=u$, (12) yields $b^{LU}\cdot b^{UR_hV}=u$, whence $b^{LU}=(b^{UR_hV})^J$. From this and another relation similarly derived we conclude that

$$L = UR_hVJU^{-1}, \qquad R = VL_gUJV^{-1}. \tag{14}$$

We substitute for L from (14) in (12), and then replace a^V by hb, b^U by ch^J, obtaining successively

$$(b^U\cdot h)^{VJ}\cdot(b^U\cdot a^V)^V = a, \qquad a^{VJ}\cdot(ab)^V = (hb)^{V^{-1}},$$

and finally

$$(ab)^V = a^V\cdot(hb)^{V^{-1}} \tag{15}$$

But (15) for $a=u$ gives $b^V=h\cdot(hb)^{V^{-1}}$, $V=L_hV^{-1}L_h$, $(VL_h^{-1})^2=I$. From the last equation on the right, and a similar one involving U, we see that we may set

$$U = SR_g, \qquad V = TL_h, \qquad S^2 = T^2 = I. \tag{16}$$

Substitution for V from (16) in (15) gives $h\cdot(ab)^T=ha^T\cdot b^T$ and therefore

$$(ab)^S = a^Sb^S, \qquad (ab)^T = a^Tb^T, \tag{17}$$

where the left-hand relation, not actually proved here, may be derived in like manner.

Equations (16) and (17) decide the issue. According to the latter, the mappings S and T are automorphisms of G. The former limits the orders of the automorphisms to one or two, and there merely remains to substitute from (16) in (11) in order to find $aob=a^Sg\cdot hb^T=a^S\cdot f\cdot b^T$, the desired conclusion.

4. **I. P. quasigroups and non-associative rings.** So far, our examples of I. P. quasigroups have been isotopic to groups. The corollary to Theorem 2 suggests that next we should construct non-associative I. P. quasigroups with (unique, two-sided) unit elements. As a first step in this direction we offer the following lemma.

LEMMA 2. *Let $A=A(+,\cdot)$ be a non-associative ring. Define the multiplicative system Q_o, consisting of the same elements as A, by*

$$xoy = x + y + x\cdot y \tag{18}$$

for every pair of elements x, y of A. Then Q_o has a unique two-sided unit element (namely the zero element 0 of A) and is associative if and only if A is associative. Necessary and sufficient conditions that Q_o be an I. P. quasigroup may be stated as follows. There must exist a one-to-one mapping J (not necessarily linear) of A into itself, such that the equations

$$x\cdot x^J = x^J\cdot x = -x - x^J \tag{19}$$

and

$$x^J\cdot(x\cdot y) = (x^J\cdot x)\cdot y, \qquad (y\cdot x)\cdot x^J = y\cdot(x\cdot x^J) \tag{20}$$

hold for all x, y of A. If these conditions are satisfied, x^J is the two-sided inverse of x in Q_o.

It should be remarked that by a non-associative ring $A(+,\cdot)$ we mean a system A which forms a commutative group under the operation $(+)$, is closed but not necessarily associative under the (single-valued) multiplication $(\cdot)$, and obeys the usual two-sided distributive law.

Proof. From (18) we see that $xo0=0ox=x$. Thus 0 is a two-sided unit of Q_o, and therefore the only such. Again, a simple computation gives

$$(xoy)oz - xo(yoz) = (x\cdot y)\cdot z - x\cdot(y\cdot z), \tag{21}$$

whence we see that Q_o is associative if and only if A is. If (19) holds true we see from (18) that $xox^J=x^Jox=0$, so that every element x of Q_o has an inverse x^J in Q_o. Conversely, if to every x there corresponds a two-sided inverse x^J in Q_o, (19) must be satisfied. Let us then assume (19) and set $z=y^J$ in (21). Thus

$$(xoy)oy^J - x = (x\cdot y)\cdot y^J - x\cdot(y\cdot y^J).$$

Hence if and only if the second equation of (20) holds true for all x, y will we have $(xoy)oy^J=x$ for all x, y. If finally we let $x=y^J$ in (21) we may link similarly the equation $y^Jo(yoz)=z$ with the first equation of (20).

Now assume that (19) and (20) are satisfied and consider the equation $xoy=z$. If x, y are given, z is determined uniquely by (18). If x, z are given, then $x^Joz=y$, so that y is uniquely determined. Similarly, if y, z are given, x is the unique element zoy^J. Hence Q_o is a quasigroup, an I. P. quasigroup. Although we have made the minimum of assumptions concerning the one-to-one mapping J, it is clear from the proof that if such a J exists at all for a given A, it is unique. Moreover, by Lemma 1, J is an anti-automorphism of Q_o, satisfying $J^2=I$.

The relation (18) might be regarded as a variation upon a method by

which G. Bol constructed a commutative Moufang quasigroup of order 81 [6, p. 426; also note pp. 430–431].

5. **The case of a linear mapping.** If we assume that the mapping J of Lemma 2 is linear, and replace x by $x+y$ in (19), we obtain

$$x \cdot y^J + y \cdot x^J = 0. \tag{22}$$

If $2x=0$ implies $x=0$ in the ring A, then (22) for $y=x$ gives $x \cdot x^J = 0$, whence from (19)

$$x^J = -x. \tag{23}$$

We shall restrict our attention to the J defined by (23).

By substitution from (23) in (20) and (22) we find

$$x^2 = 0, \qquad x \cdot y = -y \cdot x. \tag{19.1}$$

Similarly from the first equation of (20), using (23) and (19.1), we deduce

$$x \cdot (x \cdot y) = 0. \tag{20.1}$$

Moreover the second equation of (20) becomes a consequence of (19.1) and (20.1). Now replace x by $x+y$, y by z in (20.1), and derive

$$x \cdot (y \cdot z) + y \cdot (x \cdot z) = 0. \tag{24}$$

From (24) and (19.1) it follows that $x \cdot (y \cdot z) = -y \cdot (x \cdot z) = y \cdot (z \cdot x) = -z \cdot (y \cdot x) = -(x \cdot y) \cdot z$, or

$$x \cdot (y \cdot z) = -(x \cdot y) \cdot z. \tag{24.1}$$

From (24.1) we see that if $x = -x$ for all x of A, then Q_0 is associative. We therefore assume that $2x=0$ implies $x=0$.

LEMMA 3. *Let A be a non-associative ring in which $2x=0$ implies $x=0$. Assume that the equations*

$$x \cdot y = -y \cdot x \tag{25}$$

and

$$x \cdot (y \cdot z) = -(x \cdot y) \cdot z \tag{26}$$

are satisfied for all x, y of A. Then

(i) *equations* (19) *and* (20) *are true for all x, y of A, where $x^J = -x$;*

(ii) *if A is associative, $AAA=0$, and conversely;*

(iii) *the derived ring $A'=AA$ is a zero ring: $A'A'=0$;*

(iv) *the quasigroup Q_0 defined by* (18) *is a Moufang quasigroup.*

Proof.

(i) From (25) we have $x \cdot x = 0$, so (19) is satisfied. From (26) with $y=x$ we have $x \cdot (x \cdot z) = -(x \cdot x) \cdot z = 0$; hence the first equation of (20), and similarly the second, is satisfied.

(ii) If A is associative, (26) yields $(x\cdot y)\cdot z=-(x\cdot y)\cdot z$. Thus $(x\cdot y)\cdot z=0$, or $AAA=0$. The converse is evident.

(iii) Using (26) five times, we find

$$(x\cdot y)\cdot(z\cdot w) = -\,x\cdot[y\cdot(z\cdot w)] = x\cdot[(y\cdot z)\cdot w] = -\,[x\cdot(y\cdot z)]\cdot w$$
$$= [(x\cdot y)\cdot z]\cdot w = -\,(x\cdot y)\cdot(z\cdot w).$$

Thus $(x\cdot y)\cdot(z\cdot w)=0$. Since A' is the linear closure of all products $x\cdot y$, it follows that $A'A'=0$.

(iv) Since Q_0 has a unit element, we need merely verify (8), or $xo[yo(zoy)] = [(xoy)oz]oy$. By use of (18), (25) and (26) we find that each of these expressions reduces to $x+2y+z+2x\cdot y+x\cdot z$.

It would be natural at this point to attempt the construction of a non-associative A with the properties (25) and (26), and indeed the author has carried out such a project in the case that A is a linear algebra of finite order over an arbitrary field F of characteristic not equal to 2. However, it is not our intention to dwell in this paper upon problems of linear algebra, and hence the calculations will be omitted. It seems proper, nevertheless, to make a few comments upon the methods employed. Let A have finite order n over F. Let B, of order $m<n$, be a proper invariant subalgebra of A. We assume that B contains A', is itself a zero algebra, and moreover is maximal in the sense that it is contained in no larger zero algebra invariant in A. It is not difficult to show that we must take $n\geqq m+3$ if A is not to be associative, and in fact we assume $n=m+3$. Let $e_i(i=1, 2, \cdots, m)$ form a basis of B, and let e, f, g complete the basis of A. Then, after some extended considerations, we may show, first, that $m\geqq 4$ is essential, and secondly, that a proper choice of basis in B gives

$$e_1e = -\,ee_1 = e_2f = -\,fe_2 = e_3g = -\,ge_3 = e_4,$$
$$fg = -\,gf = e_1, \qquad ge = -\,eg = e_2, \qquad ef = -\,fe = e_3, \tag{27}$$

where all other products of two factors, chosen from e, f, g and those e_i for which i does not exceed four, are zero. Equations (27) are completely general (except as to choice of basis in B) for the case treated, namely $n=m+3$, A non-associative. Thus if $m=4$ $(n=7)$, (27) gives the unique non-associative A (in the sense of isomorphism) which can be obtained by this method. If $m>4$ $(n>7)$, there exist various non-isomorphic algebras A of which (27) is a partial multiplication table. One of these is obtained by assuming that all other products of two basis elements are zero.

Although we omit all supporting evidence as to the truth of the general statements of the preceding paragraph, the reader may verify for himself that the linear algebra

$$A = (e, f, g, e_i;\ i = 1, 2, \cdots, m;\ m \geqq 4) \tag{28}$$

whose multiplication table is given, except for zero products, by (27) does satisfy equations (25) and (26). It is certainly non-associative, since $e \cdot fg = ee_1 = -e_4$ while $ef \cdot g = e_3 g = +e_4$. Thus for every order $n \geqq 7$ we have exhibited a linear non-associative algebra A over F with the properties of Lemma 3. Corresponding to each such algebra there is of course an I. P. (Moufang) quasigroup Q_0, defined by (18), which is non-associative and noncommutative, and possesses a unique unit element. If F is an infinite field, Q_0 contains an infinite number of elements. But if p is an odd prime number, we may take F to be the prime field consisting of p elements. In this case Q_0 contains p^n elements (has order p^n). We are ready to state a theorem.

THEOREM 4. *Let p be any odd prime, $n \geqq 7$ be any integer. Then there exists an I. P. quasigroup, with a unit element, of order p^n. The quasigroup of order p^n which we have constructed is in fact a Moufang quasigroup, non-associative and noncommutative. Moreover, this quasigroup contains an abelian group of order p^{n-3}, and may be regarded as a non-associative extension of this group by another abelian group of order p^3.*

The last sentence of Theorem 4, which still requires proof, has been included merely for the sake of completeness. Although the proof is not difficult we shall omit it here, since it will appear as a by-product in the next section.

6. **Coset expansions.** Hausmann and Ore have given a necessary and sufficient condition [7, p. 989] for the existence of a coset expansion of a quasigroup with respect to every sub-quasigroup. For quasigroups which satisfy this condition, the same authors gave a theory of normal sub-quasigroups, and later Murdoch [8] introduced an alternative theory. Neither of these theories, however, is applicable in general to the case of I. P. quasigroups, as may be seen from the following example of order 10.

(IP)

	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	0	3	2	7	9	8	4	6	5
2	2	3	0	1	9	8	7	6	5	4
3	3	2	1	0	8	7	9	5	4	6
4	4	7	9	8	0	6	5	1	3	2
5	5	9	8	7	6	0	4	3	2	1
6	6	8	7	9	5	4	0	2	1	3
7	7	4	6	5	1	3	2	0	9	8
8	8	6	5	4	3	2	1	9	0	7
9	9	5	4	6	2	1	3	8	7	0

Here 0 is the unit element. Every element not equal to 0 generates a two-

group, every two elements not equal to 0 generate a four-group, and every three elements not equal to 0 which are not in the same four-group generate the whole quasigroup. Coset expansion with respect to a four-group is of course impossible, since four is not a divisor of ten. Expansion exists with respect to each two-group, but the product of two cosets is not in general a single coset; if $H=(0, 1)$ is the group consisting of the elements 0 and 1, then $2H=(2, 3)$, $4H=(4, 7)$, and $2H\cdot 4H=(5, 6, 8, 9)=(5H, 6H)$.

We shall now show that there does exist a satisfactory theory of coset expansions and quotient quasigroups with respect to certain sub-quasigroups in the case of quasigroups defined as in Lemma 2. Since we have been unable to verify the Hausmann-Ore condition in this case (it seems to be false even in the linear case $J=-I$) it will be necessary to proceed in detail. Thus the I. P. quasigroup $Q\equiv Q_0$ is related to the ring A via the equation

$$xoy = x + y + xy, \tag{29}$$

and there exists a one-to-one mapping J of A into itself such that the equations

$$x\cdot x^J = x^J\cdot x = -x - x^J \tag{30}$$

and

$$x^J\cdot(xy) = (x^J\cdot x)y, \qquad (yx)\cdot x^J = y(x\cdot x^J) \tag{31}$$

hold for all x, y of A.

Let B be a subring of A, and let R be the system consisting of the elements of B under the multiplication (o). From (29) it is evident that R is closed under (o), since B is closed under $(+)$ and $(\cdot)$. If B contains only a finite number of elements, or if $x^J=-x$ for all x of B, R will be an I. P. quasigroup, but in general we are in doubt as to whether R contains the inverses of its elements.

From this point onward we shall assume that B is *invariant* in A; that is, that px and xp are contained in B for every element p of B and x of A. It is then evident from (30) that $p^J=-p-p\cdot p^J$ is in R for every p of R, and thus R is an I. P. quasigroup. Moreover, if p and x are respectively in R and Q, we have

$$xop = p' + x, \tag{32}$$

where

$$p' = p + xp \tag{33}$$

is an element of B and hence of R. From (33), using (31) and (30), we find that $x^J\cdot p'=x^J\cdot p+x^J\cdot(xp)=x^J\cdot p+(-x-x^J)\cdot p=-xp$, and hence that

$$p = p' + x^J\cdot p'. \tag{33.1}$$

Conversely, if p' is an arbitrary element of R and p is defined by (33.1), we

may proceed in similar fashion back to (33). Accordingly, if for a fixed x we denote by xoR the set of all elements xop, and by $B+x$ the set of all elements $p+x$, with p in R, we have the identity

$$xoR = B + x. \tag{34}$$

By similar reasoning, $Rox = B+x$, and hence

$$Rox = xoR. \tag{35}$$

Next we wish to establish the identity

$$(xoR)o(yoR) = (xoy)oR. \tag{36}$$

Let p, q be arbitrary elements of R, so that $xop = p'+x$ and $yoq = q'+y$, where p' is given by (33) and q' is analogously defined. Then

$$(xop)o(yoq) = (p' + x) + (q' + y) + (p' + x)(q' + y) = r' + xoy, \tag{37}$$

where

$$r' = p'oq' + p'\cdot y + x\cdot q'. \tag{38}$$

Thus $(xoR)o(yoR) \subset (xoy)oR$. To see that the inequality just obtained may be replaced by (36) we set $p=0$ so that $p'=0$ and $r'=q'+x\cdot q'$. If r' be arbitrarily chosen in R we may solve this last equation for q' and hence for q in R by the methods previously explained in connection with (33) and (33.1). Hence (36) follows, as well as

$$xo(yoR) = (xoy)oR. \tag{39}$$

By the same methods we perceive that

$$(xop)o(yoq) = (xoy)or, \tag{40}$$

where

$$r = r' + (xoy)^J\cdot r', \tag{41}$$

and r' is given by (38). It would appear from (41) that the r of (40) depends in general upon both x and y, rather than upon y alone, as in the case for groups.

From (39) with y in R we see that every element of xoR defines the same coset xoR. From (34) it follows that xoR and yoR are identical if and only if they have an element in common. Finally, it is clear from (36) that the set of all distinct cosets forms an I. P. quasigroup with unit element R, in which the inverse of xoR is given by

$$(xoR)^J = x^JoR. \tag{42}$$

These considerations lead to the following:

THEOREM 5. *Let A be a non-associative ring satisfying the conditions of*

Lemma 2, *and let* $Q \equiv Q_0$ *be the I. P. quasigroup consisting of the elements of* A *under the multiplication* (18) *or* (29). *To every invariant subring* $B \subset A$ *corresponds a sub-quasigroup* $R \equiv R_0 \subset Q$, *consisting of the same elements as* B. *Coset expansion exists with respect to* R, *and the factor system* Q/R *is an I. P. quasigroup to which* Q *is homomorphic.*

COROLLARY. *If* B *contains the derived ring* A', *the factor-quasigroup* Q/R *is an abelian group.*

Proof of the corollary. If B contains A', then xy is in B for all x, y of A. In this case the element $xoy = x+y+xy$ defines the same coset as $x+y$. Accordingly Q/R is an abelian group.

This corollary settles the unproved statement of Theorem 4, provided we note in addition that if B is a zero ring then R is also an abelian group.

The relation between invariant subrings of A and what may be called normal sub-quasigroups of Q provides a suggestive basis for a theory of extensions of one I. P. quasigroup by another. It is clear of course that the direct product of two I. P. quasigroups is always an I. P. quasigroup. Aside from this remark, we shall content ourselves with a single example, in which an arbitrary I. P. quasigroup with a unit element is extended by a group of order two.

THEOREM 6. *Let* P *be an I. P. quasigroup with a unique two-sided unit* 1. *Designate the product of two elements* a, b *of* P *by* ab, *and let* a^J *be the inverse of* a. *Let* Q *consist of the elements* a, $[a]$, *under the multiplication*

$$a \cdot [b] = [a^J b], \qquad [b]a = [ba^J], \qquad [a][b] = b^J a^J. \tag{43}$$

Then Q *is an I. P. quasigroup with a unit element, containing* P *as a sub-quasigroup of index two. The inverse of* $[a]$ *is* $[a]^J \equiv [a^J]$. Q *is* (i) *a direct product of* P *and the two-group if and only if* $a^2 = 1$ *for every* a *of* P; (ii) *commutative if and only if* P *is commutative*; (iii) *a group if and only if* P *is an abelian group.*

COROLLARY. *Let* G *be a noncommutative group of finite order* g. *Then there exists a non-associative I. P. quasigroup with a unit element of order* $2^n \cdot g$ *for every integer* $n \geqq 1$.

Since in particular there exists a noncommutative group of order $2^3 = 8$, the corollary helps to round out the example of prime-power I. P. quasigroups given in Theorem 4.

Proof. In order to verify that Q is an I. P. quasigroup it is necessary to make seven calculations, of which the following is typical:

$$[a]^J \cdot ([a] \cdot [b]) = [a^J] \cdot (b^J a^J) = [a^J \cdot (b^J a^J)^J] = [a^J \cdot ab] = [b].$$

(We do not require for this calculation the fact that Q has a unit element.) Consider the other statements in order.

(i) If $a^2=1$ then $a^J=a$ for all a. Then also $ab=(ab)^J=b^Ja^J=ba$. In this case, writing $[a]=ea$, $e^2=1$, we see that (43) is the multiplication table for the direct product of P and the two-group $(1, e)$. Conversely, if Q is the direct product of P and $(1, e)$, with $[a]=ea$, the last equation of (43), taken for $b=1$, gives $ea\cdot e=a^J$, whence $a=a^J$, $a^2=1$.

(ii) The commutativity of Q of course implies that of P. If, on the other hand, P is commutative, it is clear from (43) that Q will be commutative.

(iii) If Q is a group then P is a group. Moreover P is commutative, since $(a^Jb^J)\cdot[1]=[ba]$ while $a^J\cdot(b^J\cdot[1])=[ab]$. The proof of the converse is equally simple, but a little tedious; we must show that $xy\cdot z=x\cdot yz$ for every three elements x, y and z of Q.

Added in proof: It may also be shown by similar calculations that Q is a Moufang quasigroup if and only if P is a commutative Moufang quasigroup.

7. **Other types of quasigroup.** In this section we shall consider three types of quasigroup, which we term *idempotent*, *unipotent*, and *totally symmetric* quasigroups, respectively.

DEFINITIONS. *A quasigroup is said to be idempotent if every element is idempotent: $x^2=x$ for every element x.*

A quasigroup is called unipotent if it has a unit element u and if $p^2=u$ for every element p.

A totally symmetric quasigroup (T. S. quasigroup) is one in which the relation $ab=c$ implies each of the other five relations, such as $ac=b$, obtainable by permutation of the elements a, b and c.

We note that a T. S. quasigroup is precisely a commutative I. P. quasigroup in which every element is its own two-sided "inverse." A T. S. quasigroup with a unit element is therefore unipotent; examples are the four-group and the quasigroup of order ten whose Cayley square was exhibited in §6. Conversely, a unipotent I. P. quasigroup is totally symmetric, since, first of all, every element is its own inverse, and secondly, the equation $(pq)^2=u$ implies $pq=qp$. There also exist T. S. quasigroups which are idempotent, the simplest example of which is the following:

(44)

	1	2	3
1	1	3	2
2	3	2	1
3	2	1	3

On the other hand, not every idempotent or unipotent quasigroup is totally symmetric.

The *direct product* of two quasigroups which are both idempotent or unipotent or totally symmetric is clearly of the same type as its two factors.

LEMMA 4. *There exists a process, which preserves the property of being totally symmetric, by which we may derive from an idempotent quasigroup Q of order n a unipotent quasigroup Q' of order $n+1$, and conversely.*

Since the process applies to quasigroups of infinite order, we may think of the integer n as being possibly transfinite.

Proof. Let the elements of Q be $a, b, c, \cdots$, and denote their product by $(\cdot)$. Then Q' is to consist of the same elements as Q, with the additional (unit) element u, under the multiplication (o), where

$$(45) \qquad uou = u, \qquad uoa = aou = a, \qquad aoa = u, \qquad aob = a \cdot b \qquad (a \neq b).$$

Clearly Q' is a unipotent quasigroup. Moreover if Q is totally symmetric then Q' is commutative and, indeed, is totally symmetric; for example, if a is distinct from b, then $ao(aob) = ao(a \cdot b) = a \cdot (a \cdot b) = b$.

Conversely, let Q' be a unipotent quasigroup of order greater than one, with unit element u. If the product in Q' is denoted by $(\cdot)$, let Q consist of the elements $p, q, \cdots$ of Q' distinct from u, under the multiplication (o) defined by

$$(46) \qquad pop = p, \qquad poq = p \cdot q \qquad (u, p, q \text{ not equal}).$$

Then Q is an idempotent quasigroup. If Q' is totally symmetric then every element is its own inverse in Q'. From (46), $po(pop) = pop = p$ and $po(poq) = po(p \cdot q) = p \cdot (p \cdot q) = q$. Also $poq = p \cdot q = q \cdot p = qop$. Thus Q is totally symmetric.

From the quasigroup (44) we obtain the four-group by process (45); and conversely (44) may be derived from the four-group by (46). The example of §6 was obtained via (45) from the direct product of (44) with itself.

LEMMA 5. (i) *Every finite group of odd order is isotopic to an idempotent quasigroup.* (ii) *Every commutative finite quasigroup of odd order is isotopic to an idempotent quasigroup.* (iii) *No finite commutative quasigroup of even order is idempotent.* (iv) *There exist noncommutative idempotent quasigroups of every finite even order except order two.*

COROLLARY. *There exist idempotent quasigroups of every finite order except two and (hence) unipotent quasigroups of every finite order except three.*

Proof.

(i) Let the finite group G have order $n = 2m+1$. Then if $p^2 = q^2$ we have $p = p^{2(m+1)} = q^{2(m+1)} = q$. Hence p^2, with p, runs through all the elements of G. If we define $poq = (p \cdot q)^T$, where T is the permutation of G which sends p^2 into p for all p, the quasigroup so defined is idempotent.

(ii) and (iii). We derive the proof from a remark of H. Griffin [9, p. 728]. Each element of a quasigroup Q of finite order n appears exactly n times in the Cayley square of Q. Since the Cayley square of a commutative quasigroup is

symmetric with respect to the main diagonal, each element of Q must appear an even number of times off the main diagonal. In consequence, if n is odd, each element must appear at least once, hence exactly once, on the main diagonal. In this case we see as in (i) that Q is isotopic to an idempotent quasigroup. On the other hand, if n is even each element which appears on the main diagonal appears at least twice, and hence Q is not idempotent.

(iv) First we make the trivial remarks that the unique quasigroup of order one is both idempotent and unipotent and the unique quasigroup of order two is unipotent. If n is an odd integer not less than three we shall construct a (necessarily noncommutative) idempotent quasigroup of order $n+1$. In the following, let i, j have the range $0, 1, 2, \cdots, n-1$, let the signs $(=)$ and $(<)$ have their usual meaning, and let the equation $a \equiv b$ mean that a is the smallest positive integer which is congruent to b, modulo n. Noting that we may regard the fraction $1/2$ as an integer, modulo the odd integer n, we define

$$n \cdot n = n, \qquad (n-1) \cdot 0 = n, \qquad i \cdot n \equiv i + 1/2, \qquad n \cdot i \equiv i - 1/2,$$
$$i \cdot (i+1) = n \quad \text{if} \quad i < n-1, \qquad i \cdot j \equiv (1/2)(i+j) \quad \text{if} \quad j \not\equiv i+1.$$

Without some preliminary remarks it is a little awkward to show that this definition actually gives a quasigroup. We shall be content to point out that $n \cdot n = n$ and that $i \cdot i = i$ for $i = 0, 1, 2, \cdots, n-1$. The Cayley squares corresponding to $n = 3$ and $n = 5$ are given below.

	0	1	2	3
0	0	3	1	2
1	2	1	3	0
2	3	0	2	1
3	1	2	0	3

	0	1	2	3	4	5
0	0	5	1	4	2	3
1	3	1	5	2	0	4
2	1	4	2	5	3	0
3	4	2	0	3	5	1
4	5	0	3	1	4	2
5	2	3	4	0	1	5

It is of course possible to give many other constructions similar to the above.

The corollary still remains to be proved; this is an immediate consequence of Lemmas 4 and 5.

When one is confronted with two groups, the simplest method of forming another group which contains both of these is to take their direct product. In the case of unipotent or idempotent quasigroups, other simple processes are also available. We need merely combine the two operations of Lemma 4 in a suitable manner with the operation of taking the direct product. In this connection we state and prove two lemmas.

LEMMA 6. *If P and Q are idempotent quasigroups of finite orders m and n, there exists a quasigroup R of order $(m+1)(n+1)-1 = mn+m+n$ with the*

following properties:

(i) *R contains P and Q as disjoint sub-quasigroups*;

(ii) *P and Q commute in R*;

(iii) *R is idempotent*;

(iv) *R is totally symmetric if and only if both P and Q are totally symmetric.*

COROLLARY 1. *If the P and Q of Lemma 6 are not idempotent, but merely isotopic to idempotent quasigroups, then R exists with the property* (i), *but not in general with the other properties.*

COROLLARY 2. *If P and Q are commutative quasigroups of odd orders m and n, there exists a commutative quasigroup of (odd) order $mn+m+n$ which contains P and Q as disjoint sub-quasigroups.*

COROLLARY 3. *If G and H are finite groups of odd orders m and n, there exists a quasigroup R of order $mn+m+n$ which contains G and H as disjoint sub-quasigroups which commute with one another.*

Proof of Lemma 6. Let p, q denote distinct elements of P, and a, b, distinct elements of Q. Let R consist of the m elements p, the n elements a, and the mn pairs (p, a), where

$$p\cdot a = a\cdot p = (p, a);$$

$$p\cdot(p, a) = (p, a)\cdot p = a; \qquad a\cdot(p, a) = (p, a)\cdot a = p; \tag{47}$$

$$(p, a)\cdot(q, a) = pq; \qquad (p, a)\cdot(p, b) = ab;$$

$$(p, a)\cdot(p, a) = (p, a); \qquad (p, a)\cdot(q, b) = (pq, ab).$$

It is readily verified that (47) gives the multiplication of a quasigroup with the properties of the lemma. It was derived as follows. From P and Q, via (45), we may obtain unipotent quasigroups P', Q' of respective orders $m+1$ and $n+1$. From the direct product $P'\times Q'$, via (46), we may obtain an idempotent quasigroup R_1, of order $(m+1)(n+1)-1$. Then R_1 is isomorphic to the R defined above.

Since P and Q are disjoint in R, we may apply isotopic transformations independently to P and Q without destroying the quasigroup property of R. From this fact Corollary 1 follows. The last two corollaries depend upon the fact that in order to obtain an idempotent quasigroup from a group or commutative quasigroup of odd order it is only necessary to perform a permutation (which does not destroy commutativity) upon the elements of the Cayley square itself. (Compare the proof of parts (i) and (ii) of Lemma 5.)

LEMMA 7. *If P and Q are unipotent quasigroups of finite orders m and n respectively, there exists a unipotent quasigroup R of order $(m-1)(n-1)+1 = mn-m-n+2$ with the following property. R contains $n-1$ quasigroups isomorphic to P, with only the unit element in common, and similarly $m-1$ quasi-*

groups isomorphic to Q. Moreover, R is totally symmetric if and only if both P and Q are totally symmetric.

Proof. Let u be the common unit element of P, Q and R. Besides the element u, let R contain the $(m-1)(n-1)$ elements (p, a), with $p \neq u$ in P, $a \neq u$ in Q. If p, q, u are distinct elements of P, and a, b, u, distinct elements of Q, define multiplication in R by

$$(48) \qquad \begin{aligned} (p, a)\cdot(p, a) &= u; & (p, a)\cdot(q, a) &= (pq, a);\\ (p, a)\cdot(p, b) &= (p, ab); & (p, a)\cdot(q, b) &= (pq, ab). \end{aligned}$$

Then for each a the set P_a consisting of the m elements u, (p, a) forms a sub-quasigroup of R isomorphic to P. If a is distinct from b, P_a and P_b have only the unit element in common. There exist also $m-1$ sub-quasigroups Q_p isomorphic to Q. Moreover if R is totally symmetric, so is each P_a and Q_p, and conversely.

It may be shown that (48) can be obtained by following (46) with the direct product and then (45).

The special quasigroups of this section are particularly useful in constructing quasigroups with various pathological properties, as should already be abundantly clear from Lemmas 4, 6 and 7. We mention without proof one further instance.

LEMMA 8. *Let n be any positive integer. Then an upper bound for the order of a sub-quasigroup of a quasigroup of order n is $[n/2]$ (the greatest integer in $n/2$). This upper bound is attained for every n.*

8. **Totally symmetric quasigroups.** Remembering that the totally symmetric quasigroups defined in §7 form a subset of the set of all quasigroups with the inverse property, the study of which is an important object of the present paper, we shall now consider T. S. quasigroups in more detail.

LEMMA 9. *Every commutative I. P. quasigroup is isotopic to a T. S. quasigroup.*

Proof. If Q is a commutative I. P. quasigroup, then, in the notation of Lemma 1, $L=R=J$, and J is an involutary automorphism of Q. Define Q_o by

$$(49) \qquad aob = a^J b^J = (ab)^J.$$

Then we may show without difficulty that $aob = boa$ and that $(aob)ob = a$. Hence Q_o is totally symmetric.

LEMMA 10. *A finite group G is a T. S. quasigroup if and only if it is a direct product of groups of order two.*

Proof. G is an abelian group in which every element apart from the identity has order two. Since every abelian group is a direct product of cyclic

groups, the result follows.

The result of Lemma 10, when combined with Lemma 7, readily enables us to construct unipotent T. S. quasigroups, non-isotopic to groups, of a great variety of orders. Let $n_1, n_2, \cdots, n_r$ be r integers, each a power of 2. Then, by means of $r-1$ applications of Lemma 7, we see that there exists a unipotent T. S. quasigroup of order $n+1$, where

$$n = (n_1 - 1)(n_2 - 1) \cdots (n_r - 1).$$

By this method we readily discover the existence of such quasigroups of orders 10, 22, 46, 50, and so on, and can obtain many more by taking direct products. One interesting fact about the orders of the quasigroups so obtained is that they are all even integers. This is no accident. We recall that to every unipotent T. S. quasigroup of order m there corresponds an idempotent T. S. quasigroup of order $m-1$ (Lemma 4); but there exists no commutative idempotent quasigroup of even order (cf. (iii) of Lemma 5), and therefore $m-1$ is odd.

Several problems naturally suggest themselves in connection with I. P. and T. S. quasigroups. One, which is not undertaken in the present paper, is the analysis of all unipotent T. S. quasigroups into direct products and into the "indirect products" defined by Lemma 7. Another is concerned with the isotopy of T. S. quasigroups. We might ask, for example, when two unipotent T. S. quasigroups can be isotopic, or under what circumstances an idempotent T. S. quasigroup can be isotopic to an I. P. quasigroup with a unit element. A partial answer to such questions of isotopy is given in the following theorem and its corollaries.

THEOREM 7. *Let Q be an I. P. quasigroup with a unit element u. Then the following condition is necessary and sufficient in order that Q possess an isotope Q_0 which is totally symmetric. Q must contain a fixed element g with the property that*

$$ga \cdot b = g \cdot ba \tag{50}$$

for every pair of elements a, b, of Q. If (50) *is satisfied in Q, such a Q_0 is given by*

$$aob = f(ga^J \cdot b^J g^J), \tag{51}$$

where a^J is the inverse of a in Q, and where f is any fixed element which commutes and associates with all elements of Q:

$$f \cdot ab = fa \cdot b = a \cdot fb = ab \cdot f. \tag{52}$$

Moreover, every such Q_0 is given, to within an isomorphism, by (51), *where f, g range over all elements of Q with property* (50) *and property* (52) *respectively.*

COROLLARY 1. *If Q is a group, then a necessary and sufficient condition that Q_0 be totally symmetric is that Q be abelian. In this case* (51) *becomes*

$$aob = fa^J \cdot b^J. \tag{53}$$

COROLLARY 2. *Every T. S. isotope of a commutative I. P. quasigroup (with unit element) is given, in the sense of isomorphism, by*

$$aob = f(a^J b^J), \tag{54}$$

where f satisfies (53).

COROLLARY 3. *Two unipotent T. S. quasigroups are isotopic if and only if they are isomorphic.*

COROLLARY 4. *There exists an idempotent T. S. isotope Q_0 of a commutative I. P. quasigroup Q if and only if $a^J = a^2 \equiv aa$ for every element a of Q. In this case Q_0 is given by* (54) *with $f = u$.*

COROLLARY 5. *An idempotent T. S. quasigroup Q_0 is isotopic to a group G if and only if G is the direct product of cyclic groups of order 3. In this case Q_0 is a direct power of the quasigroup* (44).

Although several of the corollaries require a certain amount of proof, no idea is involved which has not already been used in this paper. Accordingly we shall content ourselves with a proof of the theorem itself. Corollary 3, which is an easy consequence of Corollary 2, should be compared with Theorem 2. Note also that Corollary 2 gives a stronger form of Lemma 9.

Proof of Theorem 7. From (51), making use several times of (50) and (52), we find that

$$\begin{aligned} g(aob)^J = g[(gb \cdot ag^J)f^J] &= f^J[g(gb \cdot ag^J)] = f^J[(g \cdot ag^J) \cdot (gb)] \\ &= f^J[(gg^J \cdot a) \cdot (gb)] = f^J(a \cdot gb). \end{aligned}$$

Hence

$$(aob)ob = f\{[g(aob)^J] \cdot b^J g^J\} = ff^J \cdot [(a \cdot gb) \cdot (gb)^J] = a.$$

We may prove that $ao(aob) = b$ in a similar manner, using (52) along with the equation

$$b \cdot ag^J = ab \cdot g^J \tag{55}$$

which results from (50) when each side is subjected to the anti-automorphism J. Then Q_0 is an I. P. quasigroup in which $L_0 = R_0 = I$. It follows from (ii) of Lemma 1 that $aob = boa$. Thus Q_0 is commutative and hence totally symmetric. We have therefore demonstrated the sufficiency of condition (50), and may now consider its necessity.

Without loss of generality we may assume that Q_0 is a principal isotope [1, p. 698] of Q. Thus

$$aob = a^U \cdot b^V. \tag{56}$$

Where u is the unit element of Q, we define

$$g = u^U, \qquad h = u^V. \tag{57}$$

If $(aob)ob = a$, we have, successively,

$$(a^U \cdot b^V)^U \cdot b^V = a, \qquad (a^U \cdot b)^U \cdot b = a,$$

and

$$(a^U \cdot b)^U = a \cdot b^J. \tag{58}$$

From (58) with $b = u$ we find $U^2 = I$. Hence, on our replacing a by a^U, there results

$$(ab)^U = a^U \cdot b^J. \tag{59}$$

In (59) we let $a = u$ and derive

$$b^U = g \cdot b^J. \tag{60}$$

Substitution in (59) gives

$$g \cdot (ab)^J = ga^J \cdot b^J, \qquad g \cdot b^J a^J = ga^J \cdot b^J,$$

or the necessary condition (50). We have still however to encounter the f of the theorem.

By insisting that $bo(boa) = a$, we derive in a similar manner the equations

$$b^V = b^J \cdot h \tag{60.1}$$

and

$$b \cdot ah = ab \cdot h. \tag{50.1}$$

We now define

$$f = gh, \qquad h = g^J f, \tag{61}$$

and use (50) and (50.1) to find $f \cdot a = gh \cdot a = g \cdot ah = a \cdot gh = a \cdot f$, or

$$fa = af. \tag{62}$$

Similarly, $f \cdot ab = gh \cdot ab = g \cdot (ab \cdot h) = g \cdot (b \cdot ah) = (g \cdot ah) \cdot b = (gh \cdot a) \cdot b = fa \cdot b$, or

$$f \cdot ab = fa \cdot b, \qquad ab \cdot f = a \cdot bf, \tag{63}$$

where the second equation may be obtained in the same manner. Equations (52) follow from (62) and (63). Finally, from equations (56), (60), (60.1), (61) and (52), we obtain

$$aob = ga^J \cdot b^J h = ga^J \cdot (b^J \cdot g^J f) = f(ga^J \cdot b^J g^J),$$

which is (51).

We shall conclude this section with one more result.

THEOREM 8. *Let R be an idempotent T. S. quasigroup. Then a necessary and sufficient condition that R possess an isotope R_0 which is an I. P. quasigroup with a unit element is that there exist two elements p, q of R (not necessarily distinct) which yield automorphisms*:

$$p\cdot ab = pa\cdot pb, \qquad q\cdot ab = qa\cdot qb. \tag{64}$$

Every such isotope R_0 is given to within an isomorphism by

$$aob = pa\cdot qb \tag{65}$$

for some pair p, q, and has pq as its unit element.

COROLLARY. *Let Q be the idempotent T. S. quasigroup of order 2^n-1 derived via* (46) *from the abelian group G of order 2^n and type (1^n). If $n>2$, Q has no I. P. isotope with a unit element.*

The sufficiency of the condition (64) follows from (vi) of Lemma 1. We shall omit the proof of Theorem 8, since it follows the same pattern as the proofs of Theorems 1, 2, 3 and 7. In order to prove the corollary, we first note that the operation (46) only partially destroys the associative law. In fact if f, g, h are three distinct elements of G, each different from the unit element, then $f\cdot gh=fg\cdot h$ under multiplication in Q. However $fg\cdot g=f$ in Q. Let p be any element of Q. Since Q has order $2^n-1>2^2-1=3$, there exists an element a distinct from p and an element b different from each of the distinct elements pa and p. Thus $pa\cdot(p\cdot b)=(pa\cdot p)b=(ap\cdot p)b=ab\neq p\cdot ab$. It follows that Q contains no element p which yields an automorphism as in (64). In the excluded case $n=2$, Q is the quasigroup (44), which is isotopic to the cyclic group of order three.

9. **Moufang quasigroups.** We devote this section to a characterization of *Moufang* quasigroups (cf. §3, in particular equation (8)), which is given by the following theorem.

THEOREM 9. *Let Q be a quasigroup with a unit element. A necessary and sufficient condition that every isotope of Q which possesses a unit element should be an I. P. quasigroup is that Q be Moufang.*

COROLLARY. *Every isotope with a unit element of a Moufang quasigroup is Moufang.*

The corollary is a trivial consequence of Theorem 9. The proof of the theorem may be deduced from the following lemma.

LEMMA 11. *Let Q be an I. P. quasigroup with unit element u, and let Q_0 be a principal isotope of Q (with unit element fg), defined by*

$$aob = ag^J\cdot f^Jb \tag{66}$$

where f, g are fixed elements and a^J is the inverse of a in Q. Then Q_0 has the in-

verse property if and only if the equations

$$g(af\cdot gb) = (ga\cdot fg)b \tag{67.1}$$

and

$$(af\cdot gb)f = a(fg\cdot bf) \tag{67.2}$$

hold true for every pair of elements a, b of Q.

We note that, since Q has the inverse property,

$$a^{R_g^{-1}} = a\cdot g^J, \qquad a^{L_f^{-1}} = f^J\cdot a,$$

and hence (66) is the most general form of a principal isotope of Q. We merely sketch the proof of the lemma. In order to obtain (67.1) we determine c from the equation $boc=fg$, insist that $(aob)oc=a$ for all a, and then subject the result to the anti-automorphism J. The other condition follows similarly. Conversely, if equations (67) are true, we may verify that Q_o has the inverse property.

Proof of Theorem 9. Assume that Q has a unit element. If every isotope Q_o of Q which has a unit element also has the inverse property then in particular Q has the inverse property. Thus Lemma 11 applies; that is to say, a necessary and sufficient condition that every Q_o should have the inverse property is that the equations (67) hold for all f, g, a, b of Q. But (67) are equivalent to the law

$$a(bc\cdot db) = (ab\cdot cd)b, \tag{68}$$

since (68) is the same as (67.2) while (67.1) comes from (68) after an application of the anti-automorphism J. Moreover, from (68) with c put equal to u, the unit of Q, there results

$$a(b\cdot db) = (ab\cdot d)b, \tag{69}$$

or the defining relation of the Moufang quasigroups. We now must show that (69) implies (68).

Let us assume that Q is a Moufang quasigroup. That is (according to our definition), Q has a unit element u, and (69) holds true for all a, b, c. First we show that Q has the inverse property. In (69) let $a=u$; thus

$$b\cdot db = bd\cdot b. \tag{70}$$

In (70) choose d so that $bd=u$. Then $b\cdot db=b$, or $db=u$. Hence to every element a of Q there corresponds a two-sided inverse a^J such that $aa^J=a^Ja=u$. In (69) let $d=b^J$ and obtain $ab=(ab\cdot b^J)b$ or the first of the relations

$$ab\cdot b^J = a, \qquad b^J\cdot ba = a.$$

The second relation comes from (69) with $a=b^J$. Following Bol [6, p. 417,

footnote (4)] we may show that (69) implies

$$bc\cdot db = (b\cdot cd)b, \tag{71}$$

the equation which comes from (68) with $a=u$. We first need

$$(bd\cdot b)a = b(d\cdot ba), \tag{69a}$$

which results from the law (69) after an application of the anti-automorphism J. Now, by (69a),

$$b\cdot ac = b\cdot [a(b\cdot b^J c)] = (ba\cdot b)\cdot b^J c,$$

whence, by (69) and (70),

$$(b\cdot ac)b = [(ba\cdot b)\cdot b^J c]b = ba\cdot [b\cdot (b^J c\cdot b)] = ba\cdot [(b\cdot b^J c)b] = ba\cdot cb.$$

Thus $(b\cdot ac)b = ba\cdot cb$, which is equivalent to the law (71). Finally we show that (69) implies (68). In fact, by (69), (70) and (71),

$$a(bc\cdot db) = a[(b\cdot cd)b] = a[b\cdot (cd\cdot b)] = (ab\cdot cd)b.$$

This concludes the proof of Theorem 9.

A few remarks as to the background of the theory of Moufang quasigroups might prove of interest at this stage. In connection with a geometrical study R. Moufang [10] was led to the consideration of a non-associative ring A with a unit element, whose nonzero elements formed an I. P. quasigroup under multiplication. She showed [10, §II] that in view of the linearity properties of a ring, A was necessarily an alternative field, that is, an alternative ring [11] without divisors of zero. In her next paper on the subject [5] Miss Moufang pointed out that Q in fact satisfied the laws (69) and (71)—she apparently did not recognize, as did Bol [6], that (71) was a consequence of (69). Her main theorems were concerned with the facts that any two elements of a Moufang quasigroup generated a group, and that any three elements a, b, c which were associative in some order (say $a\cdot bc = ab\cdot c$) also generated a group. These results, when applied to alternative fields, yielded anew some theorems known to Max Zorn [11].

We define the isotopy of rings similarly to that for quasigroups. The mappings employed must be linear, however, as in the case of isotopy of linear algebras. According to the preceding paragraph an alternative field is a ring whose nonzero elements form a Moufang quasigroup; hence we may derive from Theorem 9 a theorem(7) on alternative fields.

THEOREM 10. *Every ring with a unit element which is isotopic to an alternative field is itself an alternative field.*

(7) Theorem 10 should be compared with a recent work by R. D. Schafer [14, Theorems 3 and 4], which gives a stronger result for the case of alternative algebras of finite order over a field.

10. **Murdoch's abelian quasigroups.** In two papers [3, 4] to which we have referred in the preceding, D. C. Murdoch has studied a class of quasigroups which are a direct generalization of abelian groups. These so-called *abelian* quasigroups obey the mild associative-commutative law

$$ab \cdot cd = ac \cdot bd. \tag{72}$$

For the various interesting properties of abelian quasigroups we refer the reader to Murdoch's papers. The object of the present section is to show briefly that every abelian quasigroup is isotopic to an abelian group, and to give an explicit construction of all such quasigroups. With the exception of the last theorem of the section, the results are essentially due to Murdoch.

LEMMA 12. *If an abelian quasigroup Q possesses a (unique, two-sided) unit element u, it is an abelian group.*

Proof. If we let $a=d=u$ in (72) we derive $bc=cb$, so that Q is commutative. Again from (72), with $c=u$, we find $ab \cdot d=a \cdot bd$, so that Q is associative. Hence Q is an abelian group.

DEFINITION. *If Q is a quasigroup and U, V are two one-to-one reversible mappings of Q on itself, we designate by $Q(U, V)$ the principal isotope Q_o given by*

$$aob = a^U \cdot b^V.$$

LEMMA 13. *Let Q be an abelian quasigroup, and let g be any fixed element of Q. Then*

(i) *$Q(R_g^{-1}, I)$ is an abelian quasigroup with unique right-unit g;*

(ii) *$Q(I, L_g^{-1})$ is an abelian quasigroup with unique left-unit g.*

Proof. (i) Let s be the uniquely determined left-unit of g, so that $sg=g$. Then, by (72),

$$ab \cdot g = ab \cdot sg = as \cdot bg.$$

Hence

$$(ab)^{R_g} = a^{R_s} \cdot b^{R_g}. \tag{73}$$

Thus, by (73),

$$[a^{R_s^{-1}} \cdot b^{R_g^{-1}}]^{R_g} = ab,$$

whence

$$(ab)^{R_g^{-1}} = a^{R_s^{-1}} \cdot b^{R_g^{-1}}. \tag{74}$$

Now define Q_o by

$$aob = a^{R_g^{-1}} \cdot b.$$

It is clear that $aog=a$, so that g is a unique right-unit. Moreover, by use of (74), (72),

$$(aob)o(cod) = (a^{R_g^{-1}} \cdot b)^{R_g^{-1}} \cdot (c^{R_g^{-1}} \cdot d) = (a^{R_g^{-1}R_g^{-1}} \cdot b^{R_g^{-1}}) \cdot (c^{R_g^{-1}} \cdot d) = (aoc)o(bod).$$

(ii) The proof of (ii) follows exactly similar lines. If we designate by r the uniquely defined right-unit of g, so that $gr = g$, we may establish the relation

$$(ab)^{L_g^{-1}} = a^{L_g^{-1}} \cdot b^{L_r^{-1}}, \tag{75}$$

by use of which the result is readily obtained.

THEOREM 11. *Let Q be an abelian quasigroup. Then every isotope of Q which possesses a unit element is isomorphic to the same abstract group G.*

Proof. Let f and g be arbitrary fixed elements of Q, let $Q_o = Q(R_g^{-1}, I)$, and define $u = fg$. Thus

$$uoa = u^{R_g^{-1}} \cdot a = fa,$$

or $L_u^o = L_f$. Then $G \equiv Q_o[I, (L_u^o)^{-1}] = Q(R_g^{-1}, L_f^{-1})$. By referring to (i) and (ii) respectively of Lemma 13 we see that Q_o and G are abelian quasigroups. But $G = Q(R_g^{-1}, L_f^{-1})$ has the unique unit element $fg = u$. Hence G is an abelian group, according to Lemma 12. In order to complete the proof we need only appeal to Theorem 2, which states that every isotope with a unit element of a group is an isomorphic group.

From the point of view of isotopy, the theory of abelian quasigroups will be complete when we show how to construct all abelian isotopes of a given abelian group. This is done in the following theorem.

THEOREM 12. *Every abelian quasigroup isotopic to an abelian group G is isomorphic to some quasigroup G_o obtained as follows:*

$$aob = f \cdot a^S \cdot b^T, \tag{76}$$

where S, T are commutative automorphisms of G and f is a fixed element of G.

Proof. (1) *Sufficiency.* From (76) and the fact that S and T are automorphisms it follows that

$$(aob)o(cod) = f \cdot f^S \cdot f^T \cdot a^{S^2} \cdot d^{T^2} \cdot b^{TS} \cdot c^{ST}. \tag{77}$$

But $ST = TS$, and hence $(aob)o(cod) = (aoc)o(bod)$.

(2) *Necessity.* Let G_o be a principal isotope of G, defined by

$$aob = a^U \cdot b^V. \tag{78}$$

If G_o is an abelian quasigroup, then $(aob)o(cod) = (aoc)o(bod)$. This relation is equivalent to

$$(ab^V)^U \cdot (c^U \cdot d)^V = (ac^V)^U \cdot (b^U \cdot d)^V. \tag{79}$$

Define the fixed elements f, g, h by

$$g = u^U, \qquad h = u^V, \qquad f = gh, \tag{80}$$

where u is the unit element of G. Also, let a^J denote the inverse of a in G. From (79) with $c=u$ we derive

$$(ab^V)^U \cdot (gd)^V = (ah)^U \cdot (b^U \cdot d)^V.$$

In the last relation we "separate the variables" a and d by multiplying each side by

$$(gd)^{VJ} \cdot (ah)^{UJ},$$

and obtain

$$(81) \qquad (ab^V)^U \cdot (ah)^{UJ} = (db^U)^V \cdot (dg)^{VJ}.$$

Since the right-hand side of (81) is independent of a, so must the left-hand side be. Similarly the right-hand side is independent of d. By equating the left side to its expression for $a=u$ we find

$$(ab^V)^U \cdot (ah)^{UJ} = b^{VU} \cdot h^{UJ}$$

or

$$(ab^V)^U = h^{UJ} \cdot (ah)^U \cdot b^{VU}.$$

Finally, on replacing b^V by b, we derive the first of the following relations, the second being similarly obtained.

$$(82) \qquad (ab)^U = h^{UJ} \cdot (ha)^U \cdot b^U; \qquad (ab)^V = g^{VJ} \cdot (ga)^V \cdot b^V.$$

Since G is commutative, we have from (82) by an interchange of a and b

$$(ha)^U \cdot b^U = (hb)^U \cdot a^U,$$

whence

$$(ha)^U \cdot a^{UJ} = (hb)^U \cdot b^{UJ} = \text{constant} = h^U \cdot g^J,$$

or

$$(83) \qquad (ha)^U = g^J \cdot h^U \cdot a^U; \qquad (ga)^V = h^J \cdot g^V \cdot a^V.$$

From (83) in (82),

$$(ab)^U = h^{UJ} \cdot g^J \cdot h^U \cdot a^U \cdot b^U = g^J \cdot a^U \cdot b^U,$$

whence

$$g^J \cdot (ab)^U = g^J \cdot a^U \cdot g^J \cdot b^U.$$

Thus if we define S, T by

$$(84) \qquad a^S = g^J \cdot a^U, \qquad a^T = h^J \cdot a^V,$$

we have

$$(85) \qquad (ab)^S = a^S \cdot b^S, \qquad (ab)^T = a^T \cdot b^T,$$

so that S, T are automorphisms of G. From (84), (78) and (80) we derive (76)

and hence (77). But if G_o is to be abelian we must have

$$b^{TS} \cdot c^{ST} = c^{TS} \cdot b^{ST}$$

or

$$b^{TS} \cdot b^{STJ} = \text{constant} = u.$$

Thus finally

$$b^{TS} = b^{ST}, \qquad ST = TS.$$

This completes the proof.

11. **Direct products of finite quasigroups.** The *direct product* $P \times Q$ of two quasigroups P and Q is defined to be the set of all ordered couples (p, q) with p in P, q in Q, under the multiplication

$$(p, q) \cdot (p', q') = (pp', qq'). \tag{86}$$

For convenience of expression let us designate by *proper sub-quasigroup* of P any sub-quasigroup distinct from P itself. Then, in the case that P, Q are groups of orders greater than one, $P \times Q$ contains proper invariant subgroups isomorphic to P and Q, but in other cases $P \times Q$ may contain no proper sub-quasigroup whatever. We shall determine necessary and sufficient conditions for the latter situation.

LEMMA 14. (i) *If P has a proper sub-quasigroup P_1, then $P \times Q$ has the proper sub-quasigroup $P_1 \times Q$.*

(ii) *If $P = P_1 \times Q$ and $Q = Q_1 \times R$ where R has order greater than one, then $P \times Q$ has a proper sub-quasigroup isomorphic to $P_1 \times Q_1 \times R$.*

Proof. (i) The set of all elements (p_1, q) with p_1 in P_1, q in Q is obviously a proper subsystem of $P \times Q$, which forms the quasigroup $P_1 \times Q$ under the multiplication (86).

(ii) The set of all elements (p_1, r, q_1, r) forms a proper sub-quasigroup of $P \times Q = P_1 \times R \times Q_1 \times R$, isomorphic to $P_1 \times Q_1 \times R$.

From part (i) of the previous lemma it is clear that if $P \times Q$ has no proper sub-quasigroups the same must be true of P and Q.

LEMMA 15. *Let P, Q be two finite quasigroups without proper sub-quasigroups. Let $P \times Q$ contain a proper sub-quasigroup R. Then*

(i) *to each element p of P there corresponds a non-null set Q_p consisting of all elements q of Q such that (p, q) is in R;*

(ii) *if $Q_p \cdot Q_{p'}$ designates the set of all elements qq' with q in Q_p, q' in $Q_{p'}$, then*

$$Q_p \cdot Q_{p'} = Q_{pp'}; \tag{87}$$

(iii) *each Q_p has the same number of elements;*

(iv) *Q_p and $Q_{p'}$ are either disjoint or identical;*

(v) *the set $\mathfrak{Q}$ consisting of all distinct sets Q_p under the multiplication* (87) *forms a quasigroup to which Q is homomorphic;*

(vi) *to each q of Q there corresponds a non-null set P_q consisting of all elements p of P such that (p, q) is in R. The sets P_q have properties analogous to those of the Q_p, and the set $\mathfrak{P}$ consisting of all distinct sets P_q forms a homomorph of P under the obvious multiplication*;

(vii) *if (p, q) is in R, then (p', q') is in R for every p' of P_q and q' of Q_p. The sets (P_q, Q_p) have properties analogous to those outlined above, and the set $\mathfrak{R}$ of all such distinct sets is a homomorph of R*;

(viii) *the three quasigroups $\mathfrak{P}$, $\mathfrak{Q}$, and $\mathfrak{R}$ are isomorphic.*

The essential point of the lemma is that the operation of matching the components p, q of each element (p, q) of R sets up a many-to-many correspondence between P and Q which gives rise to an isomorphism of the resulting homomorphs $\mathfrak{P}$ and $\mathfrak{Q}$ of P and Q.

Proof. (i) By assumption, R contains at least one element (p, q). Let p' be any element of P. Since P has no proper sub-quasigroup, there must exist some "power" $\phi(p)$ of p such that $p' = \phi(p)$. Hence

$$\phi((p, q)) = (\phi(p), \phi(q)) = (p', \phi(q)),$$

where the element on the left is obviously in R. Thus $Q_{p'}$ contains the element $\phi(q)$.

(ii) Consider the equation

$$(p, q) \cdot (p_1, q_1) = (p_2, q_2).$$

Since R is a quasigroup, if any two of the couples (p, q), (p_1, q_1), (p_2, q_2) are given as elements of R the third must be uniquely determined. It is readily seen that this fact is equivalent to (87.).

(iii) If $\phi(q)$ is any "power" of the element q of Q, designate by $\phi(q, a)$ the element obtained from $\phi(q)$ by replacing by a the q which appears at the extreme right. We first wish to show that $\phi(q, a) = \phi(q, b)$ implies $a = b$. In fact if $\phi(q) = \lambda(q) \cdot q$ this is clearly true. We then make an induction on the number of factors q which enter into $\phi(q)$, and assume that $\phi(q) = \lambda(q) \cdot \mu(q)$ where μ has fewer factors than ϕ. Then $\phi(q, a) = \lambda(q) \cdot \mu(q, a)$, so $\phi(q, a) = \phi(q, b)$ implies $\mu(q, a) = \mu(q, b)$ or $a = b$.

Now let p, p' be arbitrary elements of P, with $p' = \phi(p)$. Then, by (87),

$$\phi(Q_p) = Q_{p'},$$

and, in particular, $\phi(q, a)$ is in $Q_{p'}$ for every two elements q, a of Q_p. Since $\phi(q, a) = \phi(q, b)$ implies $a = b$, it follows that $Q_{p'}$ contains at least as many distinct elements as Q_p. By a similar argument, Q_p contains at least as many distinct elements as $Q_{p'}$, and hence the same number.

(iv) If q is in Q_p and r is an arbitrary element of P we have $q \cdot Q_r \subset Q_{pr}$. But each of the last two sets contains the same number of elements as Q_r, and hence equality must hold. If q is common to Q_p and $Q_{p'}$ we thus have

$$q \cdot Q_r = Q_{pr} = Q_{p'r} \tag{88}$$

for all r of P. Now choose r to be the uniquely defined right-unit of p', so that $p'r = p'$, and define

$$p_0 = p,\ p_1 = pr,\ p_2 = p_1 r, \cdots . \tag{89}$$

It follows from (88), (89) and the choice of r that

$$Q_{p'} = Q_{p_i}, \qquad i = 0, 1, 2, \cdots . \tag{90}$$

Since P is a finite quasigroup there exists a smallest positive integer i and some $j (0 \leqq j \leqq i-1)$ such that $p_i = p_j$. But if j is greater than zero, then $p_{i-1}r = p_{j-1}r$, whence $p_{i-1} = p_{j-1}$ with $i-1 > j-1 \geqq 0$. Since the last situation contradicts the hypotheses concerning i we must have $p_i = p_0 = p$, or $Q_{p'} = Q_p$.

(v) In view of parts (i), (ii), (iii) and (iv) of the lemma it is only necessary to show that each q of Q is contained in some set Q_p, that is, forms a component of some element (p, q) of R. But in fact, as we may show by a proof analogous to that for (i), to each q of Q there corresponds a non-null set P_q consisting of those elements p of P such that (p, q) is in R.

(vi) The proof of (vi) should be obvious from the preceding.

(vii) If (p, q) is in R, then (p', q) is in R for every p' of P_q. Moreover, for each fixed p', (p', q') is in R for every q' of $Q_{p'}$. But since $Q_{p'}$ and Q_p have the common element q we have $Q_{p'} = Q_p$. This proves the first statement of (vii). Again, if the sets (P_q, Q_p) and $(P_{q'}, Q_{p'})$ (of which we leave the precise definition to the reader) have a common element, the same must be true both of P_q and $P_{q'}$ and of Q_p and $Q_{p'}$, whence it is clear that $(P_{q'}, Q_{p'}) = (P_q, Q_p)$. The other properties analogous to those proved for the Q_p in (i)—(v) follow readily,

(viii) It is clear from (vii) that the mapping

$$P_q \rightarrow (P_q, Q_p),$$

where p is any element of P_q, is a one-to-one reversible mapping of $\mathfrak{P}$ upon $\mathfrak{R}$, with the property that

$$P_q \cdot P_{q'} \rightarrow (P_q, Q_p) \cdot (P_{q'}, Q_{p'})$$

(where of course p' is any element of $P_{q'}$). Thus $\mathfrak{P}$ is isomorphic to $\mathfrak{R}$. Similarly $\mathfrak{Q}$ is isomorphic to $\mathfrak{R}$.

This completes the proof of Lemma 15.

By adopting the terminology of G. N. Garrison [12, §4] we may throw the results of Lemma 15 into a form more suitable for use in our final theorem. For some fixed q of Q let us designate the set P_q by F. Then if q' is any other element of Q, we may choose a in Q so that $qa = q'$ and let p be any element of P_a. In this case

$$F \cdot p = P_q \cdot P_a = P_{q'},$$

and we see that every $P_{q'}$ has the form Fp for some p of P. It is easily shown that F is an *invariant complex* of P; that is, that to every pair of elements a, b of P there corresponds at least one element c of P such that

$$Fa \cdot Fb = Fc. \tag{91}$$

We shall not go into further detail regarding the theory of invariant complexes, except to remark that the quasigroup $\mathfrak{P}$ of Lemma 15 would be designated in Garrison's notation by P/F and called a *quotient quasigroup*.

THEOREM 13. *The following are necessary and sufficient conditions in order that the direct product $P \times Q$ of two finite quasigroups P and Q should contain no proper sub-quasigroup.*

(i) *P and Q must possess no proper sub-quasigroups;*

(ii) *P and Q must not possess isomorphic quotient quasigroups P/F and Q/G. (Here F and G designate invariant complexes of P and Q respectively.)*

COROLLARY. *If P and Q are two finite quasigroups of relatively prime orders, neither of which contains proper sub-quasigroups, then $P \times Q$ contains no proper sub-quasigroups.*

Proof. The necessity of (i) follows from part (i) of Lemma 14. When (i) of the theorem is assumed to hold, the sufficiency of (ii) follows from Lemma 15. Hence it only remains to consider the situation in which P contains a proper invariant complex F, and Q a similarly restricted invariant complex G, such that P/F and Q/G are isomorphic. In particular we might have P isomorphic to Q.

Let $n > 1$ be the common order of P/F and Q/G. Then F partitions P into a set of n disjoint sets $F_i = F \cdot p_i$ $(i = 1, 2, \cdots, n)$ such that to every pair of subscripts i, j there corresponds a unique subscript k for which

$$F_i \cdot F_j = F_k. \tag{92}$$

(The F_i are in fact the elements of P/F.) Similarly G partitions Q into n disjoint sets G_i. We may assume that the subscripts of the G_i have been so chosen that the correspondence

$$F_i \leftrightarrow G_i \tag{93}$$

yields an isomorphism of P/F and Q/G. Now consider the set R of all elements (p, q) of $P \times Q$ such that p and q belong for some i to F_i and G_i respectively. It is clear from (92) and (93) that R forms a proper sub-quasigroup of $P \times Q$.

This completes the proof of Theorem 13.

In the case of the corollary, the n of the above discussion would have to divide the (relatively prime) orders of P and Q. Thus $n = 1$, $F = P$, $G = Q$ and $R = P \times Q$. Hence $P \times Q$ has no proper sub-quasigroups.

We have yet to demonstrate the existence of quasigroups without proper sub-quasigroups, but in fact *such quasigroups exist of every finite order greater than two.* Let Q be an idempotent quasigroup of order $n \geqq 3$, consisting of the elements $1, 2, \cdots, n$, and let us submit the Cayley square for Q to the permutation which sends n into 1 and otherwise i into $i+1$. The quasigroup Q_0 so obtained will have the property that from any element i every element may be obtained by successive squaring; and thus Q_0 will have no proper sub-quasigroups. But in §7 we constructed idempotent quasigroups of every finite order except order two.

Now let P_1, Q_1, R be three finite quasigroups without proper sub-quasigroups, and with orders relatively prime in pairs. By the corollary to Theorem 13, the quasigroups $P = P_1 \times R$ and $Q = Q_1 \times R$ have no proper sub-quasigroups. On the other hand, the quasigroup $P \times Q$ has a proper sub-quasigroup isomorphic to $P_1 \times Q_1 \times R$, as may be seen either from Theorem 13 or from part (ii) of Lemma 14. This example exposes a misstatement made by D. C. Murdoch [3, last sentence of p. 511].

References

1. A. A. Albert, *Non-associative algebras. I. Fundamental concepts and isotopy*, Ann. of Math. (2) vol. 43 (1942) pp. 685–707; II. *New simple algebras*, loc. cit. pp. 708–723.

2. A. Suschketwitsch, *On a generalization of the associative law*, Trans. Amer. Math. Soc. vol. 31 (1929) pp. 204–214.

3. D. C. Murdoch, *Quasi-groups which satisfy certain generalized associative laws*, Amer. J. Math. vol. 61 (1939) pp. 509–522.

4. ———, *Structure of abelian quasi-groups*, Trans. Amer. Math. Soc. vol. 49 (1941) pp. 392–409.

5. R. Moufang, *Zur Struktur von Alternativkorpern*, Math. Ann. vol. 110 (1935) pp. 416–430.

6. G. Bol, *Geweben und Gruppen*, Math. Ann. vol. 114 (1937) pp. 414–431.

7. B. A. Hausmann and Oystein Ore, *Theory of quasi-groups*, Amer. J. Math. vol. 59 (1937) pp. 983–1004.

8. D. C. Murdoch, *Note on normality in quasi-groups*, Bull. Amer. Math. Soc. vol. 47 (1941) pp. 134–138.

9. H. Griffin, *The abelian quasi-group*, Amer. J. Math. vol. 62 (1940) pp. 725–737.

10. R. Moufang, *Alternativkorper und der Satz vom vollstandigen Vierseit* (D_9), Abh. Math. Sem. Hamburgischen Univ. vol. 9 (1933) pp. 207–222.

11. Max Zorn, *Theorie der alternativen Ringe*, Abh. Math. Sem. Hamburgischen Univ. vol. 8 (1931) pp. 123–147.

12. George N. Garrison, *Quasi-groups*, Ann. of Math. vol. 41 (1940) pp. 474–487.

13. A. A. Albert, *Quasigroups. I*, Trans. Amer. Math. Soc. vol. 54 (1943) pp. 507–520.

14. R. D. Schafer, *Alternative algebras over an arbitrary field*, Bull. Amer. Math. Soc. vol. 49 (1943) pp. 549–555.

University of Wisconsin,
Madison, Wis.