SIMPLE QUASIGROUPS

R. H. BRUCK

Introduction. A. A. Albert [1, II][1] has conjectured that *there exist simple loops of every finite order except order* 4. This conjecture is established in §1 by the construction of what we call *hyperabelian loops*.[2] In §2 other simple loops are constructed, in particular, loops of order $2f+1$ with subloops of order f. The concluding section of the paper is devoted to an investigation of the relationship between non-simple quasigroups (of finite or infinite order) and the loops isotopic to them (Theorem V). Theorems I and V of the paper have elsewhere been announced without proof by the author [2, §10]. For the purposes of §§1 and 2 none of the refinements of the extension theory for loops and quasigroups will be needed [1, 2, 4] and we shall be content in this introductory section with a few remarks sufficient for the proof of Lemma 1 below.

A non-empty set Q of elements $a, b, \cdots$ is said to be a *quasigroup* if (I) *to every ordered pair* $a, b \subset Q$ *there corresponds an element* $ab = c \subset Q$ and (II) *when any two of the symbols* x, y, z *of the equation* $xy = z$ *are assigned as elements of* Q *the third is uniquely determined as an element of* Q. In particular a quasigroup is called a *loop* if it possesses a (unique) unit element. Obviously every group is a loop. The *order* of a quasigroup is, by definition, its cardinal number, finite or transfinite.

If a quasigroup Q is homomorphic to a quasigroup R we may speak of R as a *proper homomorph* of Q if (i) R *is not isomorphic to* Q, (ii) R *is not a group of order one.* Correspondingly a quasigroup is *simple* if it has no proper homomorphs. This definition of simplicity is equivalent to the usual one in the case of groups, as well as to that used for finite quasigroups by G. N. Garrison [4] and to that employed by Albert [1, II] for arbitrary loops.

If a non-simple quasigroup Q has a proper homomorph R we may designate by H_p the set of elements of Q which map into the element p of R under a given homomorphism of Q upon R. Obviously H_p and H_q have common elements if and only if $p=q$. If $pq=r$, let x, y, z designate arbitrary elements of the set H_p, H_q, H_r respectively. Then,

---

Presented to the Society, April 29, 1944; received by the editors April 3, 1944.

[1] Numbers in brackets refer to the references cited at the end of the paper.

[2] The name hyperabelian loop was suggested by the fact that the multiplication table for such a loop F_G is built upon that of a commutative (or abelian) loop. When G is a cyclic group we call F_G hypercyclic.

whenever two of x, y, z are assigned in their respective sets, the third element may be uniquely determined from the equation

$$xy = z \tag{1}$$

as an element of its particular set. If we keep z fixed in (1), we derive a biunique correspondence $x \rightleftarrows y$ between the elements of H_p and H_q from which it follows that *each set H_p has the same cardinal number.* The equation (1) is equivalent to

$$H_p \cdot H_q = H_{pq}, \tag{2}$$

where, as usual, the product on the left of (2) designates the set consisting of all xy with $x \subset H_p$, $y \subset H_q$.

If Q is a loop with unit element e, then R is a loop with a unit element 1. In this case $H \equiv H_1$ is seen from (2) to be a subloop of Q; in fact a *proper* subloop, since $H \neq (e)$, Q. Moreover if $x \subset H_p$ then $H_p = xH$. In the light of these remarks the truth of parts (a) and (b) of the following lemma is evident.

LEMMA I. (a) *If, for every proper subloop H of a loop Q, there exist at least two non-identical cosets xH, yH with common elements then Q is simple.*

(b) *If a loop has no proper subloops it is simple.*

(c) *Let G be a loop of finite order g, with a subloop F of order f, where f, g are relatively prime. If every proper subloop of G is a subloop of F then G is simple.*

Part (c) of the lemma requires some additional proof. If G is homomorphic to a proper homomorph R then $H \equiv H_1$ is a proper subloop of G, $H \subset F$. Moreover if H has order h, $h \mid g$, since the disjoint sets H_p exhaust G. Again, F is homomorphic to some loop $S \subset R$, $H \subset F$ consists of all elements of F which map into the identity of S, and so $h \mid f$. Thus h divides $(f, g) = 1$. It follows that $h = 1$, G is isomorphic to R, in contradiction to the hypothesis that R is a proper homomorph of G. Therefore G is simple.

Whether Q is a loop or not we may designate any fixed set H_q as H and put each set H_p in the form $H_p = u \cdot H$. Here $u \subset H_t$, where t is the unique element of R such that $p = tq$. This is the point of view taken by Garrison [4] and later by the author [2].

1. **Hyperabelian loops.** In this section we shall prove the following theorem.

THEOREM I. *Let F be an arbitrary loop of finite order $f \geqq 2$. Let G be a commutative loop of finite order $g \geqq 3$. Then there exists a loop*

$H = F_G$ of order fg with the following properties: (i) *Every proper subloop of H is a subloop of F*; (ii) *H is simple. If $g=2$, H can be constructed with property* (i) *but not with property* (ii).

COROLLARY. *There exist simple loops of every finite order except order* 4.

The loop F_G of the theorem we call a *hyperabelian loop*.[3]

The corollary follows from Theorem I, in view of the facts that every group of prime order is simple (by Lemma I(b)!) and that the only loops of order 4 are the (non-simple) groups.

Before proceeding to the construction of the general loop F_G it will be advantageous to consider the example given by (3) below.

(3) H:

·	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	5	6	7	8	3
3	3	4	5	6	7	8	2	1
4	4	5	6	7	8	3	1	2
5	5	6	7	8	2	1	3	4
6	6	7	8	3	1	2	4	5
7	7	8	1	2	3	4	5	6
8	8	3	2	1	4	5	6	7

(4) G:

·	E	P	Q	R
E	E	P	Q	R
P	P	Q	R	E
Q	Q	R	E	P
R	R	E	P	Q

Here $F=(1, 2)$ is the cyclic group of order 2, and G is the cyclic group of order 4 given by (4). Thus $f=2$, $g=4$. If $r>f$ is an element of $H=F_G$, then any loop L containing r must contain the unit element 1. But it may be verified from (3), where $(\cdot)$ designates multiplication in H, that

(A) *if $r\cdot s=1$ for r, $s>f$ then either $s\cdot r=2$ or $r\cdot r=2$.*

Thus if L contains $r>f$ we see from (3) that L contains all elements $t\subset H$ with $t>f$. It then follows that $L\supset F$, $L=H$. Thus, in this case, the only proper subloop of H is F itself. But $3\cdot F$ contains the ele-

[3] See the previous footnote.

ments 3, 4 and $4 \cdot F$ contains the elements 4, 5. Hence H is simple, by virtue of Lemma I(a).

In the general case, if $n>4$ is a composite integer, then n has at least one representation of the form $n=fg$ with $f \geqq 2$, $g \geqq 3$. Let G be any arbitrary commutative loop of order g, with elements $E, P, Q, \cdots$, where E is the unit element, and construct the multiplication table for G, as for example in (4). The Cayley square which is formed by deleting the sideline and headline of the multiplication table for G we shall call the *G-square*. Let F be an arbitrary loop of order f (not necessarily commutative), and designate the elements of F by $1, 2, \cdots, f$, where 1 is the unit element of F. Finally, let the elements $1, 2, \cdots, f, f+1, \cdots, n$ designate the elements of the proposed quasigroup $H=F_G$, where 1 is the unit element. In the sideline and headline of the multiplication table for G replace E by a column and row consisting of the numbers $1, 2, \cdots, f$, similarly P by the numbers $f+1, f+2, \cdots, 2f$, and so on, so that the numbers $1, 2, \cdots, n$ are now written in order in sideline and headline.

We shall first give a very simple construction of the multiplication table for $H=F_G$ (in terms of the multiplication for G, modified as above) and then indicate possible generalizations. In the G-square replace that element E which stands in the first row and column of the G-square by the F-square. Thus, as illustrated by (3), the upper left hand corner of the partially constructed multiplication table for H gives the table for F. Now replace each of the remaining elements $P, Q, \cdots$ of the first column of the G-square by a square (not a Cayley square) of f rows and columns, in the following manner: Think of the column formed by $P, Q, \cdots$ as a rectangle consisting of f columns and $n-f$ rows; in the first column write the elements $f+1, f+2, \cdots, n$ in order, and repeat these numbers, in cyclic permutation, in each successive column. (Thus the ith column, $2 \leqq i \leqq f$, consists of the elements $f+i-1, f+i, \cdots, n, f, f+1, \cdots, f+i-2$ written in that order.) Next, replace the element P, wherever it appears in the G-square, by the square which has replaced P in the first column of the G-square, and do the same for Q, and so on, but not for E.

At this stage of the construction it should be clear that 1 has been made the unit element of H and, moreover, that no row or column of the H-square contains the same number more than once. (The second fact has been ensured by use of the Cayley square of a loop G.) Again, if the element E appears below the main diagonal in place (i, j), $1<j<i$, replace E by *any Cayley square* $C_{i,j}$ *of order* f, *formed from the elements* $1, 2, \cdots, f$ (for example, by the F-square itself).

Since G is commutative, E must also appear above the main diagonal, in place (j, i); and this time we replace E by the Cayley square $C'_{i,j}$ *derived from* $C_{i,j}$ *by interchanging the numbers* 1 *and* 2. We have thus partially assured the condition (A); in fact *if* $r \cdot s = 1$ *with* $r > f$, $s > f$, *and if* r, s *differ by at least* f, *then* $s \cdot r = 2$. Finally, suppose that E appears on the main diagonal of the G-square, in place (i, i) with $i > 1$, as will happen when G has an element of order two; in this case, replace E by a Cayley square $C_{i,i}$, formed from the elements $1, 2, \cdots, f$, *such that* 2 *appears in every place on the main diagonal, of* $C_{i,i}$.[4] Thus *if* $r \cdot s = 1$ *with* $r > f$, $s > f$, *and if* r, s *differ by less than* f, *then* $r \cdot r = 2$. The multiplication table of H is now complete, and satisfies condition (A); moreover the H-square is a Cayley square, in that each of the numbers $1, 2, \cdots, n$ appears exactly once in each row and column.

In view of condition (A), any subloop S of H which contains an element $r > f$ must contain the element 2. Also, by construction, $n \cdot 2 = f+1$ and $s \cdot 2 = s+1$ for $f < s < n$; or (to say the least!)

(B) *the mapping* $r \to r \cdot 2$ *(for* $f < r \leqq n$*) is a permutation of the elements* $f+1, \cdots, n$ *which maps no element into itself.*

It follows that S contains all the elements $f+1, \cdots, n$ and hence every element of H. This much is true even in the excluded case $g = 2$, and hence the constructed $H = F_G$ has property (i) of Theorem I for $g = 2$.

As A. A. Albert has shown [1, II], every loop of order $n = 2f$ $(f > 1)$ which contains a subloop of order f is non-simple. Thus once more we assume $g \geqq 3$. What we have to say here depends essentially upon the construction of the first f columns of the H-square; so we note that

(C) *assuming* $f < r \leqq f(g-1)$, *the first* f *elements of the* r*th row of the* H*-square are, in order,* $r, r+1, \cdots, r+f-1$.

Although we gave the construction by columns, the truth of (C) is readily verified. Now let L be a proper subloop of H, so that $L \subset F$, L has order $l \leqq f$. Then, using (C), we see that the coset $(f+1) \cdot L$ contains the element $f+1$ and, in addition, $l-1 \geqq 1$ of the elements $f+2, \cdots, 2f$. Let r be the greatest of the elements contained in $(f+1) \cdot L$; hence $f+1 < r \leqq 2f \leqq f(g-1)$. Then, using (C) again, we see that $r \cdot L$ contains r and other elements $t > r$, but not the element $f+1$. Thus $(f+1) \cdot L$ and $r \cdot L$ are distinct cosets with the common element r. By reference to Lemma I(a) we verify that H is a simple loop.

[4] Any Cayley (or latin) square, formed from the elements $1, 2, \cdots, f$, can be converted into a Cayley square with 2 down the main diagonal by suitable permutations of the rows.

Before attempting to generalize the construction of the loop $H=F_G$ we should realize that properties (i) and (ii) of Theorem I contain the essential features of the construction. For (i) we used conditions (A) and (B), and for (ii), condition (C). Now the only important fact about the element 2 used in (A) and (B) is that it is an element of F but not the identity; but to replace 2 by another element would not effect the construction in an essential manner. If 1 is to be the unit element of H we must have $1\cdot i=i\cdot 1=i$ for all i of H, but, aside from this restriction, condition (C) may be relaxed as regards the order in which the first f elements of the rth row appear. Then, if the first f columns of H have been completely filled in, and if the various E's have been replaced by Cayley squares as described above, the rest of the H-square may be filled in any manner, subject only to the obvious restrictions that 1 be the unit element of H and that each of the numbers $1, 2, \cdots, n$ appear exactly once in each row and column of the H-square.

Taking the case that F is the cyclic group of order $f=3$ and that G is the four-group ($g=4$) we give below two simple hypercyclic loops $H=F_G$. That given by (5) was constructed according to the first, or simpler, method, and that given by (6), with the conditions relaxed.[5] When f and g are both fairly large, considerably more freedom of construction is of course possible, without destroying the essential features (i) and (ii) of the hyerabelian loops.

(5)

·	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	3	1	5	6	7	8	9	10	11	12	4
3	3	1	2	6	7	8	9	10	11	12	4	5
4	4	5	6	2	3	1	10	11	12	7	8	9
5	5	6	7	1	2	3	11	12	4	8	9	10
6	6	7	8	3	1	2	12	4	5	9	10	11
7	7	8	9	10	11	12	2	3	1	4	5	6
8	8	9	10	11	12	4	1	2	3	5	6	7
9	9	10	11	12	4	5	3	1	2	6	7	8
10	10	11	12	7	8	9	4	5	6	2	3	1
11	11	12	4	8	9	10	5	6	7	1	2	3
12	12	4	5	9	10	11	6	7	8	3	1	2

[5] Note that the differences between (5) and (6) appear in the second and third rows and in the blocks of elements down the main diagonal.

(6)

·	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	3	1	6	7	8	9	10	11	12	4	5
3	3	1	2	5	6	7	8	9	10	11	12	4
4	4	5	6	2	1	3	10	11	12	7	8	9
5	5	6	7	3	2	1	11	12	4	8	9	10
6	6	7	8	1	3	2	12	4	5	9	10	11
7	7	8	9	10	11	12	3	1	2	4	5	6
8	8	9	10	11	12	4	2	3	1	5	6	7
9	9	10	11	12	4	5	1	2	3	6	7	8
10	10	11	12	7	8	9	4	5	6	3	2	1
11	11	12	4	8	9	10	5	6	7	1	3	2
12	12	4	5	9	10	11	6	7	8	2	1	3

2. **Other simple loops.** Elsewhere [3, p. 38] the author has announced without proof the following result.

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

A. A. Albert [1, II] has published a proof of the first statement of this lemma, and has shown moreover that if a quasigroup Q of even order $n=2m$ has a sub-quasigroup of order m then Q is non-simple. We shall now construct the most general *loop* G of odd order $n=2m+1$ which has a subloop F of order $m>1$. (In case $m=1$, G is the cyclic group of order 3.)

THEOREM II. *Let F be an arbitrary loop of finite order $m>1$, consisting of the elements $1, 2, \cdots, m$, with unit element 1. Let G be a system of order $n=2m+1$, consisting of the elements $1, 2, \cdots, n$, closed under a single-valued multiplication, and containing the loop F as a multiplicative subsystem of order m. Let the multiplication table for G be given by*

(7)

·		
	A	B_1
	C_1	D_1

where it is understood that the sideline and headline each contain the

numbers $1, 2, \cdots, m, m+1, \cdots, n$ *written in natural order. If* A *denotes the Cayley square for* F *then the following conditions are necessary and sufficient in order that* G *be a loop*:

(i) B_1 *must be obtainable by deleting the last row of a Cayley square* B *on the elements* $m+1, \cdots, n$, *of which the first row consists of those elements in natural order.*

(ii) C_1 *must be obtainable by deleting the last column of a Cayley square* C *on the elements* $m+1, \cdots, n$, *of which the first column consists of those elements in natural order.*

(iii) D_1 *must be obtainable from a Cayley square* D *on the elements* $0, 1, 2, \cdots, m$, *in the following manner. Each of the elements* $1, 2, \cdots, m$ *occupies the same position in* D_1 *as in* D. *The latter is partially determined by* B *and* C, *in that if* i (*for* $m+1 \leqq i \leqq n$) *appears in the row numbered* r_i *of the last column of* C *and in the column numbered* c_i *of the last row of* B $(1 \leqq r_i, c_i \leqq m+1)$ *then* 0 *must appear at the intersection of the* r_i*th row and* c_i*th column of* D. *Moreover* i *must appear at the intersection of the* r_i*th row and* c_i*th column of* D_1.

COROLLARY. *For every integer* $m>1$, *there exists a loop* G *of order* $n=2m+1$, *with the following properties*: (a) G *contains an arbitrary loop* F *of order* m. (b) *Every proper subloop of* G *is a subloop of* F. (*By Lemma* I(c), G *is simple.*)

With a few fairly obvious changes Theorem II can be altered to give the construction of the most general *quasigroup* of order $n=2m+1$ with an arbitrary sub-quasigroup of order m.

PROOF OF THEOREM II. Since G is to be a loop with subloop F, the unit element of G must coincide with 1, the unit of F. Hence the first row of B_1 (first column of C_1) must consist of the elements $m+1, \cdots, n$ in natural order. Since A is a Cayley square on the elements $1, 2, \cdots, m$, none of these elements can appear in any row or column of B_1 or of C_1. In particular B_1 consists of m rows and $m+1$ columns formed from the $m+1$ elements $m+1, \cdots, n$. In view of the fact that G is to be a loop, there can be no repetitions in any row or column of B_1; hence each column of B_1 lacks exactly one of the elements $m+1, \cdots, n$, clearly a different one for each column. Thus the missing elements form a uniquely determined final row, which, when added to B_1, yields a Cayley square B on the elements $m+1, \cdots, n$, the first row of which contains the elements in natural order. Thus condition (i) is necessary in order that G be a loop, and similar considerations show the necessity of (ii). Now if the element i $(m+1 \leqq i \leqq n)$ is missing from the r_ith column of B_1, or appears in

the corresponding column of the last row of B, then i must appear somewhere in the r_ith column of D_1. Similarly if the same i is missing from the c_ith row of C_1, it must appear in the c_ith row of D_1. Finally, since this i can appear at most once in each row and column of C_1, it must appear at the intersection of the r_ith row and c_ith column of D_1, and nowhere else in D_1. Moreover, since the elements $1, 2, \cdots, m$ appear nowhere in B and C, each must appear exactly once in each row and column of D_1. Thus if D be obtained from D_1 by replacing each $i>m$ by 0, D must be a Cayley square; it follows that (iii) is necessary in order that G be a loop.

Conversely, let B, C be Cayley squares with first row and final column respectively consisting of the elements $m+1, \cdots, n$ in natural order, let D be a Cayley square on the elements $0, 1, 2, \cdots, m$ with 0 appearing in the places prescribed by (iii), and let B_1, C_1, D_1 be derived from B, C, D as described in the theorem. Then, in the inside of the multiplication table (7), each of the elements $1, 2, \cdots, n$ will appear exactly once in each row and column, inasmuch as A is the given Cayley square for F. Thus G will be a quasigroup, and, in fact, a loop, since it will have unit element 1. Thus the conditions (i), (ii) (iii) are sufficient.

When it comes to the actual problem of constructing G we find it necessary to give further consideration to the relationships between the Cayley squares B, C and D. If B and C are given, subject to the mild restrictions of (i) and (ii), then the positions of the element 0 in D are fixed. But if D' is an arbitrary Cayley square on $0, 1, \cdots, m$ we may permute the rows and columns of D' in order to bring 0 into the prescribed places, and hence there is no difficulty about constructing D. Suppose, on the other hand, that D and B are given arbitrarily. Since D is given, the positions of 0 are fixed in D. Since the last row of B is given, the positions of the elements $m+1, \cdots, n$ in D_1 are fixed, and hence the last column of C is fixed. Thus the first and last columns of C are fixed, and we are faced with the problem of constructing a Cayley square of order $m+1 \geqq 3$ with two given columns. When $m=2$ the remaining column of C is uniquely determined, but whether the construction is always possible for $m>2$ is not obvious.

There is no difficulty in constructing a loop G with the properties of the corollary. For example, let B be the symmetric Cayley square in which successive rows are obtained by cyclic permutations of the first row, and let C be identical with B. Then D will have 0 down the main diagonal, and D_1 will have down the main diagonal the elements $n, m+1, m+2, \cdots, n-1$ in that order. If $i>m$ is any element of G not in F, the elements $i_0=i$, $i_1=i\cdot i$, $i_2=i_1\cdot i_1$, $\cdots$, $i_m=i_{m-1}\cdot i_{m-1}$ will

comprise all elements of G which are not in F, and the subloop generated by i will coincide with G. This establishes the corollary. If F is commutative, the G so constructed will be commutative if and only if D is commutative; but D can be commutative [5, p. 728, or 3, pp. 35–36] if and only if its order $m+1$ is even, or if m is odd, $m=2k+1>1$. Hence we have obtained the following result.

THEOREM III. *Let k be any positive integer, and let F be an arbitrary commutative loop of order $2k+1$. Then there exists a simple commutative loop G of order $4k+3$, with the property that every proper subloop of G is a subloop of F. (In particular F is a subloop of G of maximum possible order.)*

It should be noted conversely that if the G of Theorem II is commutative then C must be the transpose of B, and hence D must be a symmetric Cayley square of order $m+1\geqq 3$ with 0 down the main diagonal. But this can only happen for $m=2k+1\geqq 3$, and so Theorem III gives a "best possible" result of its kind.

We conclude this section with a result due to H. Griffin [5, p. 731].

THEOREM IV. *Let I_n designate a commutative loop of order $n>1$, which contains no proper subloops. Then*

(i) *I_{2m} does not exist for $m\neq 1$;*

(ii) *I_2, I_3 and I_5 are cyclic groups;*

(iii) *a non-associative I_n exists for every odd integer $n>5$.*

COROLLARY. *When I_n exists, it is simple.*

For the proof of Theorem IV we refer the reader to Miss Griffin's paper,[6] which also contains many other useful constructions. The corollary follows from Lemma I(b).

3. **The extension theory for quasigroups.** In another paper [2, §10] we have defined the extension $P=(H, Q)$ of a set H by a quasigroup Q. It will be convenient to repeat the definition. If H is a set of order m and Q a quasigroup of order n (m, n being finite or transfinite) then P is constructed so as to be a quasigroup of order mn. We suppose that to every pair p, q of elements of Q there has been defined a quasigroup $H_{p,q}$ consisting of the elements of H. No connection is

[6] There seems to be a slight slip in the third sentence of Miss Griffin's construction, which could be corrected by replacing her sentence by these: "Now interchange the elements of the last row, except for the last element, with the principal diagonal elements immediately above them, and alter the last column correspondingly to preserve commutativity. Also change the headline and sideline of the multiplication table to agree respectively with the first row and column of the table."

postulated between the ordered products of a, b in the various $H_{p,q}$, and we denote this product in $H_{p,q}$ by[7] $\phi_{p,q}(a, b)$.

We define $P=(H, Q)$ to be the set product of H and Q, namely the set of all couples (a, p) with $a \subset H$, $p \subset Q$, where $(a, p)=(b, q)$ if and only if $a=b$, $p=q$. The ordered product of $x=(a, p)$ and $y=(b, q)$ is given by $x \cdot y=z=(c, r)$ with

$$c = \phi_{p,q}(a, b), \qquad r = pq. \tag{8}$$

There is now no difficulty in verifying that P is a quasigroup. Moreover, if we designate by H_p the set of all (a, p) with $a \subset H$, then

$$H_p \cdot H_q = H_{pq}, \tag{9}$$

whence it follows that *the set* $\mathfrak{Q}$ *of all sets* H_p *forms a quasigroup isomorphic to* Q, and P *is homomorphic to* $\mathfrak{Q}$. If, conversely, a quasigroup P is homomorphic to a quasigroup S, it is proved in [2] that P is isomorphic to an extension (H, Q) with Q isomorphic to S. Finally, *an extension* (H, Q) *is a loop with unit element* $(e, 1)$ *if and only if*: (i) Q *is a loop with unit* 1; (ii) $H_{1,1}$ *is a loop with unit* e; (iii) e *is a left unit for every* $H_{1,q}$ *and a right unit for every* $H_{p,1}$. Condition (iii) clearly implies (ii). In case P is a loop, A. A. Albert calls $H_{1,1}$ a *normal divisor*, and H may be taken to be identical with $H_{1,1}$.

It is our purpose in this section to supply a proof of the following theorem, previously announced in [2].

THEOREM V. *Let* $P=(H, Q)$ *be a quasigroup extension of a set* H *by a quasigroup* Q. *Then every loop isotopic to* P *is isomorphic to some extension* $P_0=(H_0, Q_0)$ *where* Q_0 *is a loop isotopic to* Q *and* H_0 *is a set (which may be taken to be a loop) of the same order as* H.

COROLLARY. *Every isotope of a simple loop is simple.*

PROOF. If f, g are fixed and x, y arbitrary elements of P, consider the system P_0 with multiplication

$$xoy = xR_g^{-1} \cdot yL_f^{-1}. \tag{10}$$

Here the operators L_f^{-1}, R_g^{-1} designate respectively the inverses of the one-to-one mappings

$$x \to xg = xR_g, \qquad y \to fy = yL_f \tag{11}$$

of P upon itself. It is known [1, 3] that P_0 is a loop and has unit ele-

[7] The only difficulties to be found in the proof of Theorem V of this section are those of notation. It has been found advantageous in this instance to replace certain notations previously used by the author [2, 3] by those recently adopted by Albert [1].

ment $f \cdot g$ (this much may be verified without difficulty from (10) and the definition of a loop), and, moreover, that every loop isotopic to P is isomorphic to a loop P_0 defined for some f and g of P. Hence our proof will consist merely in relating (10) to the fact that $P = (H, Q)$.

If p, q are any elements of Q we define the one-to-one mappings R_p, L_p of Q upon itself by

$$pq = pR_q = qL_p. \tag{12}$$

Similarly, if a, b are any elements of H we define one-to-one mappings $R_a^{p,q}$, $L_b^{p,q}$ of the quasigroup $H_{p,q}$ upon itself by

$$\phi_{p,q}(a, b) = aR_b^{p,q} = bL_a^{p,q}. \tag{13}$$

Assuming that

$$f = (\alpha, u), \qquad g = (\beta, v), \qquad x = (a, p), \qquad y = (b, q), \tag{14}$$

we now may show that

$$xR_g^{-1} = (aV_p^{-1}, pR_v^{-1}), \qquad yL_f^{-1} = (bU_q^{-1}, qL_u^{-1}) \tag{15}$$

where V_p, U_q are one-to-one mappings of H upon itself, defined by

$$\begin{aligned} V_p &= R_\beta^{p',v}, & p' &= pR_v^{-1}, \\ U_q &= L_\alpha^{u,q''}, & q'' &= qL_u^{-1}. \end{aligned} \tag{16}$$

In fact, where g, x are given by (14), the definition of product in $P = (H, Q)$ yields $xR_g = x \cdot g = (\phi_{p,v}(\alpha, \beta), pv) = (aR_\beta^{p,v}, pR_v)$. The inverse mapping R_g^{-1} is uniquely defined; hence if we take it to be given by (15.1) then $x = xR_gR_g^{-1} = (aR_\beta^{p,v}, pR_v)R_g^{-1} = (aR_\beta^{p,v} \cdot V_{pv}^{-1}, p)$. It follows that R_g^{-1} has been correctly defined if and only if

$$V_{pv} = R_\beta^{p,v}.$$

In this last relation we replace p by $pR_v^{-1} = p'$ and obtain (16.1). Similarly we may verify that L_f^{-1} is correctly given by (15.2) if and only if U_q is given by (16.2).

Before proceeding, let us note that V_p depends not only upon p but upon the fixed element $g = (\beta, v)$. A similar remark holds for U_q.

By use of (10), (8), (15) and (16), a direct calculation gives

$$xoy = (\overset{0}{\phi}_{p,q}(a, b), poq) \tag{17}$$

where

$$poq = pR_v^{-1} \cdot qL_u^{-1} \tag{18}$$

and

$$\phi^{0}_{p,q}(a, b) = \phi_{p',q''}(aV_p^{-1}, bU_q^{-1}). \tag{19}$$

Now (18) defines a loop Q_0, isotopic to Q, and with unit element $u \cdot v \equiv 1$. (Compare the corresponding remarks above about (10) and P.) Moreover, for each fixed pair p, q of elements of Q_0, (19) defines a quasigroup $H^0_{p,q}$ consisting of the elements of H under the multiplication $\phi^0_{p,q}(a, b)$; in fact if p, q are given then p', q'' are determined by (16), and the equation $\phi^0_{p,q}(a, b) = c$, or

$$\phi_{p',q''}(aV_p^{-1}, bU_q^{-1}) = c,$$

enables us to determine any one of a, b, c uniquely once the other two are given. It is indeed evident that *each quasigroup $H^0_{p,q}$ is isotopic to the corresponding quasigroup $H_{p',q''}$*. Since the $H^0_{p,q}$ are quasigroups we see from (17) that P_0 is an extension (H_0, Q_0) of the set $H_0 \equiv H$ by the loop Q_0. But P_0 is itself a loop, and hence the proof of Theorem V is complete.

In view of (10) we know that the unit element of P_0 is

$$(e, 1) \equiv f \cdot g = (\alpha, u)(\beta, v) = (\phi_{u,v}(\alpha, \beta), uv). \tag{20}$$

It would seem of interest to give a direct proof of the facts that $H^0_{1,1}$ is a loop with unit element e, and that e is a left unit for every $H^0_{1,q}$ and a right unit for every $H^0_{p,1}$. Now, from (16), $1' = uv \cdot R_v^{-1} = u$ and $1'' = uv \cdot L_u^{-1} = v$. Moreover $eV_1^{-1} = \phi_{u,v}(\alpha, \beta) \cdot [R^{u,v}_\beta]^{-1} = \alpha$ and $eU_1^{-1} = \phi_{u,v}(\alpha, \beta)[L^{u,v}_\alpha]^{-1} = \beta$. Hence, by (19), (16) and (13),

$$\phi^{0}_{1,q}(e, b) = \phi_{u,q''}(\alpha, bU_q^{-1}) = bU_q^{-1} \cdot L_\alpha^{u,q''} = b$$

and

$$\phi^{0}_{p,1}(a, e) = \phi_{p',v}(aV_p^{-1}, \beta) = aV_p^{-1} \cdot R_\beta^{p',v} = a$$

for all a, b. In particular we also have $\phi^0_{1,1}(a, e) = \phi^0_{1,1}(e, a) = a$.

References

1. A. A. Albert, *Quasigroups*. I, Trans. Amer. Math. Soc. vol. 54 (1943) pp. 507–519; II, loc. cit. vol. 55 (1944) pp. 401–419.

2. R. H. Bruck, *Some results in the theory of linear non-associative algebras*, Trans. Amer. Math. Soc. vol. 56 (1944) pp. 141–199.

3. ———, *Some results in the theory of quasigroups*, Trans. Amer. Math. Soc. vol. 55 (1944) pp. 19–52.

4. G. N. Garrison, *Quasi-groups*, Ann. of Math. vol. 41 (1940) pp. 474–484.

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

University of Wisconsin