ON LOOPS WITH A SPECIAL PROPERTY[1]

RAFAEL ARTZY

1. The loop G is defined, as usual, as a multiplicative system having a unit u, and such that in the equation $xy=z$ any two of x, y, z uniquely determine the third. Let the right inverse element of any $x\in G$ be x', so that $xx'=u$.

We postulate a special *property* π: $xy\cdot x'=y$ for any x and y in G.

Such loops are interesting in connection with a generalization [1] of those plane webs whose study inspired the notion of the Moufang loop [2]. The problem which has arisen in this respect[2] was the independence between the "inverse properties" $y\cdot y'x=x$ and $xy\cdot y'=x$ (equivalent to those defined in [3]) and our property π. Since each of the "inverse properties" implies the equality of the right and left inverses of any element, the existence of a loop with the property π and different right and left inverses of at least one element will be sufficient to prove the independence.

In the study of our loops we use the concept of a *cycle of inverses* (in short: *cycle*), i.e. a finite sequence of elements $x_1, x_2, \cdots, x_n$ such that $x_k'=x_{k+1} \bmod n$. The number n will be called the *length* of the cycle. A length of 1 or 2 implies identity of right and left inverses in this cycle; groups thus have only cycles of length 1 or 2. Our loops, if finite, consist only of cycles, and every element belongs exactly to one cycle.

In the following we shall deal mainly with the cycles and their lengths.

2. The following properties are simple deductions from the postulates. In the following x, y, z denote elements of G.

$$x\cdot yx' = y. \tag{2.1}$$

PROOF. Let $y=xz$. In view of π, $xz\cdot x'=yx'=z$; left multiplication by x yields $x\cdot yx'=y$.

$$(xy)' = x'y'. \tag{2.2}$$

PROOF. By π we have $(xy\cdot x')(xy)'=x'$. Hence $y\cdot(xy)'=x'$. Right multiplication by y' gives $y(xy)'\cdot y'=x'y'$. By virtue of π this becomes

Presented to the Society, September 3, 1954; received by the editors March 12, 1954 and, in revised form, July 20, 1954.

[1] The author wishes to express his thanks to the referee for his helpful suggestions.

[2] *Added in proof.* Cf. my paper, *Loops and generally situated 4-webs*, Scient. Publ. of Israel I. T. vol. 6 (1955).

$$(xy)' = x'y'.$$

Let T map each element upon its right inverse, so that π becomes $xy \cdot xT = y$. The left inverse of any x is xT^{-1}. In this notation we derive from (2.2) by iteration

$$(xy)T^n = xT^n \cdot yT^n \tag{2.3}$$

for all n where n is an integer. Thus the T^n are automorphisms of G.

3. THEOREM 1: *A loop G with the property π cannot consist only of u and a finite number m of cycles of equal finite length n, unless n is a factor of $2m$.*

PROOF. Let $x_1, x_2, \cdots, x_m$ be fixed elements of G, one from each cycle. Every element of G, except u, may be written in the form of x_iT^k. Then

$$x_p \cdot x_qT^{k+1} = x_rT^{f_p(k,q)}, \qquad k \neq 0 \text{ when } p = q, \tag{3.1}$$

for a suitable function f_p. By π, (3.1) implies

$$x_rT^{f_p(k,q)} \cdot x_pT = x_qT^{k+1}$$

or, by (2.3),

$$x_r \cdot x_pT^{1-f_p(k,q)} = x_qT^{k+1-f_p(k,q)},$$

that is

$$f_r(-f_p(k, q), p) = k + 1 - f_p(k, q). \tag{3.2}$$

Let us regard each cycle as an additive cyclic group Z_i of integers; x_i corresponds to the zero element and x_iT^k to k. Let the sum of the elements of each Z_i be s. Since $k+(-k)=0$ for every k in Z_i, $2s=0$.

In order to find the sum of (3.2) for all k, q, p ($k \in Z_q$; $q=1, \cdots, m$; $p=1, \cdots, m$) we have to consider first the range of values of r in (3.1). When k and q run through all possible values, p remaining fixed, the r.h.s. of (3.1) has to represent all elements of G except u and x_p. Thus r runs through all values $1, \cdots, m$; $f_p(k, q)$ runs for every r, except $r=p$, through all elements of Z_r, and in the case $r=p$ through $1, \cdots, n-1$ only. When summing, the absence of the zero element in the range of r has no importance, so we have

$$\sum_q \sum_k f_r(-f_p(k, q), p) = \sum_j \sum_i f_i(j, p).$$

If we sum for all p also, we get

$$\sum_p \sum_q \sum_k f_r(-f_p(k, q), p) = \sum_p \sum_j \sum_i f_i(j, p) = \sum_p \sum_q \sum_k f_p(k, q)$$

because the order of summation is irrelevant. Thus the r.h.s. and the last term of the l.h.s. are canceled out. Now we have only to sum the first two expressions of the r.h.s. of (3.2):

$$0 = m^2 s + m(mn - 1),$$

or

$$0 = 2m^2 s + 2m^2 n - 2m.$$

But, as $2s = 0$, this is possible only if n divides $2m$.

COROLLARY. *If a loop with the property π consists only of u and one cycle, the length of the cycle is* 1 *or* 2, *i.e. right and left inverses are identical.*

The two cases of the corollary are represented by the cyclic groups C_2 and C_3, respectively. 3 cycles of length 1 give Klein's "Vierergruppe," 2 cycles of length 2 yield C_5. On the other hand, the author has not succeeded in constructing a loop which consists only of u and cycles of equal finite length greater than 2.

THEOREM 2. *There exist infinitely many nonisomorphic loops of infinite order with the property π, consisting only of u and elements of the form xT^k, where x is a fixed element and k ranges through all the integers.*

PROOF. In the notation of Theorem 1 we have now $m = 1$. Formulae (3.1), (3.2) become

$$x \cdot xT^{k+1} = xT^{f(k)}, \tag{3.3}$$

$$f(-f(k)) = k + 1 - f(k). \tag{3.4}$$

Each of the following equations implies the others because of (3.4):

$$f(k) = j, \qquad f(-j) = k + 1 - j, \qquad f(j - k - 1) = -k. \tag{3.5}$$

Let Z be the additive group of integers. The values of f, for nonzero arguments in sets of three, may be defined by stages according to the following rules: If, at some stage, k is the numerically smallest nonzero integer (the positive, if there are two) for which $f(k)$ has not been defined, define (3.5) to be true where j is the numerically smallest nonzero integer (the positive, if there are two) consistent with the requirements: (a) k, $-j$, $j-k-1$ are distinct, nonzero, not previously used as arguments of f; (b) j, $k+1-j$, $-k$ have not been used previously as values of f. The first three stages are:

$$f(1) = -2, \qquad f(2) = 4, \qquad f(-4) = -1;$$

$$f(-1) = 3, \qquad f(-3) = -3, \qquad f(3) = 1;$$
$$f(-2) = 5, \qquad f(-5) = -6, \qquad f(6) = 2.$$

These rules may be varied in obvious ways (e.g. by choosing arbitrarily different values for $f(1)$) to give infinitely many distinct effective constructions.

Let G_f consist of Z and an additional element u, with multiplication (o) defined as suggested by (3.3):

$$u \circ u = u, \qquad u \circ k = k, \qquad k \circ (k+1) = u,$$

and

$$k \circ (j+1) = k + f(j-k) \qquad \text{for } j \neq k.$$

Then G_f has the required properties.

Suppose two such loops to be isomorphic without having equal f's. Let the first loop be G_f with elements xT^k, and the other one G_g with elements yT^k. The operation T is an invariant of the isomorphism. If x corresponds to a fixed yT^h of G_g, then $x \cdot xT^{k+1} = xT^{f(k)}$ implies

$$(yT^h) \cdot (yT^h)T^{k+1} = (yT^h)T^{f(k)}.$$

By (2.3) this becomes

$$y \cdot yT^{k+1} = yT^{f(k)},$$

and hence

$$f(k) = g(k) \qquad \text{for all } k.$$

Thus different f's define nonisomorphic G_f's, and there exist infinitely many nonisomorphic G_f's.

THEOREM 3. *The unit element and the elements of a cycle of length n, together with the elements of all the cycles whose lengths are factors of n, form a subloop.*

PROOF. Elements remain unaltered by T^n if and only if they belong to the cycles described in the theorem. Let x, y be such elements. Then their product also has the same property: By (2.3), $(xy)T^n = xT^n \cdot yT^n = xy$.

THEOREM 4. *If a loop with the property π has a cycle of length n, greater than 2, it has another cycle whose length is a factor of n.*

PROOF. By the corollary to Theorem 1 the cycle together with u cannot form a subloop. Thus the cycle contains at least one pair of (not necessarily distinct) elements x, y whose product is in a different

cycle. But $(xy)T^n = xy$; hence the product belongs to a cycle whose length divides n.

By Theorem 4 we get a *sequence of cycles* containing all cycles whose lengths form a sequence of integers where each is a factor of the next one. Such a sequence of cycles may imply by Theorem 3 a corresponding sequence of subloops $H_1 \subset H_2 \cdots \subset H_k$ such that each subloop contains its predecessors as (not necessarily proper) subloops. The number of subloops need not necessarily equal the number of cycles because several cycles of equal length yield only one corresponding subloop. The sequence of cycles whose lengths are, respectively, $n_1, n_2, \cdots, n_r$ has the following properties: Each n is a factor of all subsequent n's. Either n_1 has the value 1 or 2, or $n_1 = n_2$; in the latter case the requirements of Theorem 1 have to be satisfied: if $n_1 = n_2 = \cdots = n_m \neq n_{m+1}$, then n_1 has to be a factor of $2m$. (Since, as can be shown without difficulty, there is no loop consisting only of u and two cycles of length 4, $m \geqq 3$, if such a loop can be constructed at all.)

THEOREM 5. *A loop with the property π cannot consist only of u and two wholly distinct sequences of cycles.*

PROOF. Let x, y be elements of the last cycle of each sequence, and n and p the lengths of the cycles to which x, y, respectively, belong. Since n and p are lengths of cycles in different sequences, neither is a factor of the other. Hence

$$(xy)T^n = x \cdot yT^n \neq xy,$$
$$(xy)T^p = xT^p \cdot y \neq xy,$$

and xy cannot belong to either sequence, a contradiction.

THEOREM 6. *If a loop of infinite order with the property π contains finite cycles, then u and all elements of all cycles form a subloop.*

PROOF. Let p be the product of the lengths of all the cycles. Then T^p leaves invariant all the elements of the cycles, but not the other elements. Thus the requirements for Theorem 3 are satisfied.

4. The construction of loops with more than one sequence of cycles is rather cumbersome. Here are some examples with one sequence. C_4 has 2 cycles of lengths 1, 2; C_6 has 3 cycles of lengths 1, 2, 2. The following multiplication tables describe one loop with cycle-lengths 2, 6 (with one subloop of order 3) and two loops with cycle-lengths 1, 8 (each with one subloop of order 2). Comparison of the last two tables yields

THEOREM 7. *Loops of finite order with the property π which are of*

identical structure as regards the number of cycles and their length, need not be isomorphic.

u	1	2	3	4	5	6	7	8
1	2	*u*	6	5	8	7	4	3
2	*u*	1	4	7	6	3	8	5
3	6	8	7	*u*	1	5	2	4
4	3	7	5	8	*u*	2	6	1
5	8	4	2	6	3	*u*	1	7
6	5	3	8	1	7	4	*u*	2
7	4	6	1	3	2	8	5	*u*
8	7	5	*u*	2	4	1	3	6

u	1	2	3	4	5	6	7	8	9
1	*u*	8	9	2	3	4	5	6	7
2	4	7	*u*	6	9	5	8	3	1
3	5	1	8	*u*	7	2	6	9	4
4	6	5	1	9	*u*	8	3	7	2
5	7	3	6	1	2	*u*	9	4	8
6	8	9	4	7	1	3	*u*	2	5
7	9	6	2	5	8	1	4	*u*	3
8	2	4	7	3	6	9	1	5	*u*
9	3	*u*	5	8	4	7	2	1	6

u	1	2	3	4	5	6	7	8	9
1	*u*	8	9	2	3	4	5	6	7
2	4	7	*u*	8	6	5	9	3	1
3	5	1	8	*u*	9	7	6	2	4
4	6	5	1	9	*u*	2	8	7	3
5	7	4	6	1	2	*u*	3	9	8
6	8	9	5	7	1	3	*u*	4	2
7	9	3	2	6	8	1	4	*u*	5
8	2	6	4	3	7	9	1	5	*u*
9	3	*u*	7	5	4	8	2	1	6

References

1. Rafael Artzy, *Eigenschaften von ebenen Viergeweben allgemeiner Lage*, Math. Ann. vol. 126 (1953) pp. 336–342.

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

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

Israel Institute of Technology