Compositio Mathematica

Edgar G. Goodaire
D. A. Robinson

Loops which are cyclic extensions of their nuclei

Compositio Mathematica, tome 45, nº 3 (1982), p. 341-356
<http://www.numdam.org/item?id=CM_1982__45_3_341_0>

COMPOSITIO MATHEMATICA, Vol. 45, Fasc. 3, 1982, pag. 341–356

LOOPS WHICH ARE CYCLIC EXTENSIONS OF THEIR NUCLEI

Edgar G. Goodaire* and D.A. Robinson

0. Introduction

In this paper a loop L is said to be a cyclic extension of its nucleus N provided that N is normal in L and that the quotient loop L/N is a group of prime order[1]. For such a loop L the authors are concerned with the structure of L, which is not associative since $|L/N| > 1$, as well as with inherent properties of the group N. In this regard, the main result (see Theorem 1.1) gives a necessary and sufficient condition for a group N to be the nucleus of a loop L which is a cyclic extension of N with $|L/N| = p$, where p is any prescribed prime. (The reader will see that Theorem 1.1 stands in contrast to an analogous group-theoretic result of M. Hall [6, p. 225] on cyclic extensions.) It will be interesting to note that only groups N with nontrivial centers can serve as such nuclei. For $p > 2$ every such group N is the nucleus of such a loop (see Corollary 1.4). For $p = 2$ the situation is quite different; although Abelian groups

*This author wishes to thank most sincerely the faculty and staff of the School of Mathematics at the Georgia Institute of Technology for many kindnesses during his 1979–80 visit and also the Natural Sciences and Engineering Research Council of Canada for its support, Grant No. A9087.

[1] Throughout this paper the authors assume that the reader is familiar with the basic results, terminology, and notation of loop theory (see, for instance, the comprehensive works of V.D. Belousov [1] and R.H. Bruck [2] as well as the less comprehensive, but very readable, article by R.H. Bruck [What is a loop? Studies in Modern Mathematics, M.A.A. (1963), 59–99]). Loops, for the most part, are multiplicatively written here, and so the authors speak merely of a loop L, only resorting to the more cumbersome notation $(L,\cdot)$ to avoid possible confusion in the presence of more than one binary operation. In the same vein, the authors shall frequently, in order to circumvent excessive verbiage, make concessions like the following: "the group N is the normal nucleus of some loop L" means "there exists a loop L whose nucleus is normal and whose nucleus is isomorphic to N".

0010-437X/82030341-16$00.20/0

with exponent different from 2 as well as certain carefully selected groups which are not Abelian (see the remarks following Corollary 1.4) are index 2 nuclei of a loop, there do exist groups which cannot be index 2 nuclei of any loop.

The authors' present investigation was motivated to a great extent by their search (see the authors [5]) for finite G-loops[2] of composite order $n > 5$ which are not groups. It is not surprising, therefore, that in §2 attention is focused on G-loops. It is shown that, by imposing some additional conditions (see Theorem 2.1) on the loops studied in §1, examples of G-loops can be obtained.

1. Structure

The left, middle, and right nuclei of a loop L are denoted by N_λ, N_μ, and N_ρ respectively and are defined by $N_\lambda = \{x \in L \mid x(yz) = (xy)z$ for all $y, z \in L\}$, $N_\mu = \{y \in L \mid x(yz) = (xy)z$ for all $x, z \in L$, and $N_\rho = \{z \in L \mid x(yz) = (xy)z$ for all $x, y \in L\}$. The nucleus N of a loop L is then defined by $N = N_\lambda \cap N_\mu \cap N_\rho$.

THEOREM 1.1: *Let N be a group whose identity element is denoted by 1 and let p be a prime. Then there exists a loop L with normal nucleus N such that L/N is a group of order p if and only if there exist elements $k_{ij} \in N$ for integers i, j with $1 \leq i, j \leq p-1$ and an automorphism θ of N so that*

$$k_{1j} = 1 \quad \text{if } j < p-1, \tag{1}$$

$$k_{ij} \in Z(N), \text{ the center of } N, \quad \text{if } i + j < p, \tag{2}$$

$$n\theta^p = k_{ij} n k_{ij}^{-1} \quad \text{if } i + j \geq p, \tag{3}$$

and, furthermore, at least one of the following three conditions holds:

$$k_{ij} \neq 1 \text{ for some } i \text{ and } j \text{ with } i + j < p, \tag{4}$$

$$k_{ij} \neq k_{1,p-1} \text{ for some } i \text{ and } j \text{ with } i + j \geq p, \tag{5}$$

$$k_{1,p-1}\theta \neq k_{1,p-1}. \tag{6}$$

PROOF: Let N be a group whose identity element is denoted by 1 and let p be a prime.

[2] The term *G-loop* seems to have originated with V.D. Belousov [1] and is used to designate any loop which is isomorphic to all of its loop isotopes.

(I) For the sufficiency, assume that N has an automorphism θ and elements k_{ij} so that (1), (2), (3) hold and at least one of (4), (5), (6) holds. Now let G be a cyclic group of order p and let a be a generator of G. Let L be the Cartesian product $N \times G$ and define a product for L by

$$(n_1, a^i)(n_2, a^j) = (n_1 \cdot n_2\theta^i \cdot k_{ij}, a^{i+j}) \tag{7}$$

with the understanding that $k_{i0} = k_{0j} = 1$ for all i, j. To show that any set L on which a binary operation has been defined is a quasi group one needs only establish that whenever any two of x, y, z (not necessarily distinct) are given as elements in L the third can be uniquely determined in L so that $xy = z$. In the present context, $(n_i, a^i)y = (n_2, a^j)$ has the unique solution $y = (n, a^s)$ where $0 \le s \le p-1$ with $s \equiv j - i \pmod p$ and $n = (n_1^{-1} \cdot n_2 \cdot k_{is}^{-1})\theta^{-i}$. Likewise, the equation $x(n_1, a^i) = (n_2, a^j)$ has the unique solution $x = (m, a^t)$ where $0 \le t \le p-1$ with $t \equiv j - i \pmod p$ and $m = n_2 \cdot k_{ti}^{-1} \cdot n_1^{-1}\theta^t$. Using the same symbol 1 for the identity element of G (i.e., $1 = a^0$), one can easily verify that $(1, 1)$ is the identity element of L. Hence, L is a loop relative to the binary operation given in (7).

Now let $N(L) = \{(n, 1) \mid n \in N\}$. It is clear that $N(L)$ is a subloop of L and that N and $N(L)$ are isomorphic. It will now be shown that $N(L)$ is the nucleus of L. For this purpose let $x = (n, 1) \in N(L)$ and let $y = (n_1, a^i)$ and $z = (n_2, a^j)$ be any elements in L. Then, by a direct computation, one sees that $x(yz) = (xy)z = (nn_1 \cdot n_2\theta^i \cdot k_{ij}, a^{i+j})$ and also that $(yx)z = (n_1 \cdot n\theta^i \cdot n_2\theta^i \cdot k_{ij}, a^{i+j})$ and $y(xz) = (n_1 \cdot (nn_2)\theta^i \cdot k_{ij}, a^{i+j})$. But since θ^i is an automorphism of N it follows that $(yx)z = y(xz)$. Thus, it is seen that $N(L) \subseteq N_\lambda \cap N_\mu$ where N_λ and N_μ are, respectively, the left and middle nuclei of L. Now note that

$$y(zx) = (n_1 \cdot (n_2 \cdot n\theta^j)\theta^i \cdot k_{ij}, a^{i+j})$$

whereas

$$\begin{aligned} (yz)x &= (n_1 \cdot n_2\theta^i \cdot k_{ij},\ a^{i+j})(n, 1) \\ &= \begin{cases} (n_1 \cdot n_2\theta^i \cdot k_{ij} \cdot n\theta^{i+j},\ a^{i+j}) & \text{if } i + j < p \\ (n_1 \cdot n_2\theta^i \cdot k_{ij} \cdot n\theta^{i+j-p},\ a^{i+j-p}) & \text{if } i + j \ge p. \end{cases} \end{aligned}$$

If $i + j < p$, then condition (2) together with the fact that θ^i is an automorphism of N guarantees that $y(zx) = (yz)x$. If $i + j \ge p$, condition (3) permits one to write $k_{ij} \cdot n\theta^{i+j-p} \cdot k_{ij}^{-1} = (n\theta^{i+j-p})\theta^p = n\theta^{i+j} = (n\theta^j)\theta^i$, and so, in this case, it is also true that $y(zx) = (yz)x$. Thus, one now has $N(L) \subseteq N_\rho$, where N_ρ is the right nucleus of L. Putting together what is available at this point, one concludes that $N(L) \subseteq N_\lambda \cap N_\mu \cap N_\rho$.

For convenience in this paragraph let $D(L) = N_\lambda \cap N_\mu \cap N_\rho$. It was established above that $N(L) \subseteq D(L)$. To show that $N(L)$ is, in fact, the nucleus of L it will suffice to show that $D(L) \subseteq N(L)$. Suppose that $D(L) \not\subseteq N(L)$ and let $w = (n, a^i)$ be an element such that $w \in D(L)$ but $w \notin N(L)$. Necessarily one has $i \not\equiv 0 \pmod p$. Note that $(n^{-1}, 1) \in N(L)$ implies that $(n^{-1}, 1)w = (1, a^i) \in D(L)$. Then $(1, a^i)^2 = (k_{ii}, a^{2i})$ must also be in $D(L)$. But then $(k_{ii}^{-1}, 1) \in N(L)$ implies that $(k_{ii}^{-1}, 1)(1, a^i)^2 = (k_{ii}^{-1}, 1)(k_{ii}, a^{2i}) = (1, a^{2i})$ is also in $D(L)$. Continuing in this fashion (i.e., successively multiplying on the left by $(1, a^i)$), one can show that $(1, a^{ti}) \in D(L)$ for all integers t. Since $i \not\equiv 0 \pmod p$ there is an integer t so that $ti \equiv 1 \pmod p$. Hence, $(1, a)$ must be an element of $D(L)$. But $D(L)$ is associative, and so powers of $(1, a)$ are well-defined. Using (1) in conjunction with $(1, a)^{i+1} = (1, a)(1, a)^i$ and proceeding inductively, one obtains

$$(1, a)^i = \begin{cases} (1, a^i) & \text{if } i < p \\ (k_{1,p-1}\theta^{i-p}, a^i) & \text{if } i \geq p. \end{cases}$$

Now, if i, j, and $i+j$ are all less than p, it follows that $(1, a^{i+j}) = (1, a)^{i+j} = (1, a)^i(1, a)^j = (1, a^i)(1, a^j) = (k_{ij}, a^{i+j})$ and so in this case $k_{ij} = 1$. If $i + j = p$, it follows that $(k_{1,p-1}, 1) = (1, a)^p = (1, a)^i(1, a)^j = (k_{ij}, 1)$ and so in this case $k_{ij} = k_{1,p-1}$. Also $(1, a)(1, a)^p = (1, a)^p(1, a)$ implies that $k_{1,p-1}\theta = k_{1,p-1}$, and so finally, if $i + j > p$ (with $i < p$ and $j < p$), it follows that $(k_{1,p-1}, a^{i+j}) = (k_{1,p-1}\theta^{i+j-p}, a^{i+j}) = (1, a)^{i+j} = (k_{ij}, a^{i+j})$ and so $k_{ij} = k_{1,p-1}$. Hence, none of (4), (5) or (6) holds and so a contradiction has been reached. Thus, $N(L) = N_\lambda \cap N_\mu \cap N_\rho$ and so $N(L)$ is the nucleus of L.

Now let $x = (n, a^i)$ be any element in L and let $y = (n_1, 1)$ be any element in $N(L)$. Then it is clear that $yx = x(n_2, 1)$ where $n_2 = (n^{-1} \cdot n_1 \cdot n)\theta^{-i}$. Hence, one sees that $N(L)x \subseteq xN(L)$. Likewise, one can show that $xN(L) \subseteq N(L)x$. Since $N(L)$ is the nucleus of L and $xN(L) = N(L)x$ for all $x \in L$, it follows that $N(L)$ is a normal subloop of L. At this point it is easy to see also that $L/N(L)$ is isomorphic to G. Identifying $(n, 1)$ and n and thereby writing N for $N(L)$, one sees that N is the nucleus for a loop L so that N is normal in L and L/N is a group of order p.

(II) For the necessity, assume that N is the nucleus of some loop L so that N is normal in L and L/N is a group of order p. Now select a to be any element of L such that $a \notin N$. For any integer n define a^n recursively as follows: $a^0 = 1$, $a^{i+1} = a \cdot a^i$. Since $(Na)^i = Na^i$ and L/N is associative, it follows that $(Na^i)(Na^j) = Na^{i+j}$ or Na^{i+j-p} according as $i + j < p$ or $i + j \geq p$ respectively. Hence, there exist elements $k_{ij} \in N$, for $0 \leq i,\ j \leq p-1$, such that

$$a^i \cdot a^j = \begin{cases} k_{ij}a^{i+j} & \text{if } \ i+j<p \\ k_{ij}a^{i+j-p} & \text{if } \ i+j \geq p. \end{cases}$$

Note that $k_{1j} = 1$ for $j < p-1$. Thus, condition (1) holds. Note also that $k_{0j} = k_{i0} = 1$ for $0 \leq i,\ j \leq p-1$. Since N is normal in L, it follows that $aN = Na$, and so for each $n \in N$ there is a unique $n\theta \in N$ so that $an = n\theta \cdot a$. One can show easily that θ is a bijection of N. Also note that $a^2 n = a \cdot an = a \cdot n\theta \cdot a = n\theta^2 \cdot a^2$ for all $n \in N$ and, more generally, that $a^i n = n\theta^i \cdot a^i$ for all integers i and all $n \in N$. In fact, paying close attention as to which elements are in the nucleus N of L, one can show that $n_1 a^i \cdot n_2 a^j = (n_1 \cdot n_2\theta^i)a^i a^j$ and that

$$n_1 a^i \cdot n_2 a^j = \begin{cases} n_1 \cdot n_2\theta^i \cdot k_{ij} \cdot a^{i+j} & \text{if } \ i+j<p \\ n_1 \cdot n_2\theta^i \cdot k_{ij} \cdot a^{i+j-p} & \text{if } \ i+j \geq p \end{cases}$$

for all $n_1, n_2 \in N$ and all i, j with $0 \leq i,\ j \leq p-1$. Since N is the nucleus of L, it now follows that $(n_1 n_2)\theta \cdot a = a(n_1 n_2) = (an_1)n_2 = (n_1\theta \cdot a)n_2 = n_1\theta \cdot an_2 = n_1\theta(n_2\theta \cdot a) = (n_1\theta \cdot n_2\theta) \cdot a$ for all $n_1, n_2 \in N$. Thus, appealing to the cancellation property of loops, one sees that $(n_1 n_2)\theta = n_1\theta \cdot n_2\theta$ for all $n_1, n_2 \in N$. Thus, the bijection θ of N is, in fact, an automorphism of N.

If $i+j<p$, it follows that $(k_{ij} \cdot n\theta^{i+j})a^{i+j} = k_{ij} \cdot a^{i+j}n = k_{ij}a^{i+j} \cdot n = a^i a^j \cdot n = a^i(n\theta^j)a^j = (n\theta^j)\theta^i a^i a^j = (n\theta^{i+j} \cdot k_{ij})a^{i+j}$ for all $n \in N$. Thus, with cancellation, one sees that $k_{ij} \cdot n\theta^{i+j} = n\theta^{i+j} \cdot k_{ij}$ for all $n \in N$. But, since θ^{i+j} is a surjection of N, it is clear that $k_{ij} \in Z(N)$ and condition (2) is established. Now, if $i+j \geq p$, one shows similarly that $n\theta^{i+j} \cdot k_{ij} = k_{ij} \cdot n\theta^{i+j-p}$. Applying θ^p to both sides and appealing to the surjectivity of θ^{i+j}, condition (3) is established.

One can show by a tedious, but straightforward argument, that the denial of (4), (5), and (6) implies that a must be an element of N, which contradicts how a was selected. Specifically, one shows that, with neither (4) nor (5) holding, $a \in N_\lambda \Leftrightarrow a \in N_\mu \Leftrightarrow a \in N_\rho \Leftrightarrow k_{1,p-1}\theta = k_{1,p-1}$. Consequently, at least one of (4), (5), and (6) must hold and the proof of Theorem 1.1 is complete.

It seems worth observing at this point that *the loop L of Theorem* 1.1 *cannot be power-associative.* Suppose, on the contrary, that L is power-associative. It is then immediate from the way the k_{ij}'s arise that $k_{ij} = 1$ if $i+j<p$ and $k_{ij} = k_{1,p-1}$ if $i+j \geq p$. But in the presence of power-associativity it is also true that $a^p \cdot a = a \cdot a^p$ which, in turn, guarantees that $k_{1,p-1} \cdot a = a \cdot k_{1,p-1} = k_{1,p-1}\theta \cdot a$ and, by cancellation, that $k_{1,p-1} =$

$k_{1,p-1}\theta$. Hence, none of (4), (5), and (6) can hold and a contradiction has been reached.

Theorem 1.1 has direct bearing on a variety of situations as is indicated by the corollaries below.

Although the nucleus of a Moufang loop is normal (see R.H. Bruck [2, p. 114]), it is not known whether or not the same is true for the nucleus of a Bol loop. (For basic information concerning Bol loops and their relation to Moufang loops, see D.A. Robinson [9].) In this regard the following corollary is significant.

COROLLARY 1.2: *Let p and q be primes, let L be a Bol loop of order pq which is not a group, and let N be the nucleus of L. If N is normal in L, then $|N| = 1$.*

PROOF: Since $|N|$ divides $|L|$ (see R.H. Bruck [2, p. 92]) and $N \neq L$, it follows that $|N| = 1$, p, or q. Suppose that $|N| \neq 1$. There is no loss of generality if one takes $|N| = q$. Then L/N is a Bol loop (every homomorphic image of a Bol loop which is a loop is also a Bol loop) of prime order p. But a Bol loop of prime order is a group (see R.P. Burn [3]) and, hence, is power-associative. But L/N being power-associative is in conflict with the observation above. Consequently, one must conclude that $|N| = 1$.

In view of the preceding corollary any search for Bol loops of order pq with p and q prime having non-normal nuclei would have to be restricted to such loops with non-trivial nuclei. Recently Harald Niederreiter and Karl Robinson [7] constructed entire classes of Bol loops of order pq for some pairs of distinct odd primes p and q. Unfortunately, all of their loops have trivial nuclei.

Recall that a loop L is said to satisfy the *weak inverse property* provided that $xy \cdot z = 1$ if and only if $x \cdot yz = 1$. A loop L is called here *completely weak* provided that every loop isotopic to L satisfies the weak inverse property. Such loops have been studied by J. Marshall Osborn [8].

COROLLARY 1.3: *If L is a completely weak loop of order pq where p and q are odd primes (not necessarily distinct), then L is a group.*

PROOF: Let L be any loop which satisfies the hypothesis of this corollary and let N denote the nucleus of L. Then N is normal in L and L/N is a Moufang loop (see J. Marshall Osborn [8]). If $|N| = 1$, then L is a Moufang loop of order pq and so L must be a group (see Orin Chein [4]). Also, if $N = L$, it is obvious that L is a group. Since $|N|$ divides $|L|$

(see again R.H. Bruck [2, p. 21]), the only cases left to consider are $|N| = q$ and $|N| = p$. Without loss of generality, now let $|N| = q$. With $|N| = q$, the loop L/N is a Moufang loop of order p and, hence, L/N is a group (see again Orin Chein [4]). Thus, Theorem 1.1 is available. Since $|L/N| = p$ it is clear that for any $a \in L$ all p^{th} powers of a are in N. Suppose that for some $a \in L$ with $a \notin N$ one of the p^{th} powers of a is not the identity element of N. Then this p^{th} power of a generates the group N and, since Na generates L/N, one sees that a generates L. Thus, L is a completely weak loop which is generated by one element. As such L must be a homomorphic image of Osborn's free completely weak loop on one generator (see J. Marshall Osborn [8]). But Osborn's loop has all squares in the nucleus and so also must L. Thus, it is clear that if for some $a \notin N$ any p^{th} power of a is not the identity element of N then L/N has exponent 2 and order $p > 2$, which is quite impossible for the group L/N. Thus, it must be true that all p^{th} powers of all $a \in L$ with $a \notin N$ are equal to the identity of N. Then it follows immediately that a^i is well-defined for $0 \leq i \leq p$ and so, by (8), all $k_{ij} = 1$. Thus, none of (4), (5), and (6) can hold. In other words, the case $|N| = q$ cannot occur and the proof of Corollary 1.3 is complete.

In speculating as to the existence of G-loops of order $3q$ which are not groups, R.L. Wilson [11(c)] asks whether or not there might exist loops of order $3q$ which satisfy an identity of Eric Wilson [10] without being groups. It suffices to assume that q is an odd prime. Since loops which satisfy Eric Wilson's identity are known to be completely weak (see Eric Wilson [10]), the preceding corollary shows that any such loop of order $3q$ with q an odd prime must be a group. Thus, in such situations the Eric Wilson identity must be abandoned. The existence of G-loops of order $3q$ is taken up again in the next section.

If Theorem 1.1 is to be of any use in the actual construction of loops L which are cyclic extensions of given groups N, it is essential that one be able to select groups N which satisfy the conditions listed in Theorem 1.1. In other words what groups N can serve as normal nuclei of loops L with $|L/N| = p$ with p a prescribed prime? This question is easily answered if $p > 2$.

COROLLARY 1.4: *Let p be a prime with $p > 2$. Then a group N satisfies the requirements set forth in Theorem* 1.1 *if and only if N has a non-trivial center.*

PROOF: Let N be a group which satisfies (1), (2), and (3) of Theorem 1.1. Suppose that $|Z(N)| = 1$. Then with $p > 2$ and (2) holding it is clear that (4) cannot be satisfied. Note that with $Z(N)$ trivial one must conclude that $a = b$ whenever $a, b \in N$ and $ana^{-1} = bnb^{-1}$ for all $n \in N$. This last observation in conjunction with (3) shows that (5) cannot hold. Now, using (3), one sees that

$$(k_{1,p-1}\theta) \cdot n \cdot (k_{1,p-1}\theta)^{-1} = (k_{1,p-1} \cdot n\theta^{-1} \cdot k_{l,p-1}^{-1})\theta = n\theta^{-1}\theta^{p}\theta = n\theta^{p}$$
$$= k_{1,p-1} \cdot n \cdot k_{l,p-1}^{-1}$$

for all $n \in N$. Thus, $k_{1,p-1}\theta = k_{1,p-1}$ and so (6) does not hold. Consequently, in the presence of (1), (2), (3) for at least one of (4), (5), and (6) to hold it is necessary that the center of N be non-trivial.

Conversely, let N be any group with a non-trivial center. Select k_{12} (note that $p > 2$) to be any element in $Z(N)$ with $k_{12} \neq 1$. For all i, j with $i \neq 1$ and $j \neq 2$ let $k_{ij} = 1$ and select θ to be the identity automorphism of N. Then N satisfies the requirements of Theorem 1.1 and the proof of Corollary 1.4 is complete.

When $p = 2$ the situation is quite different because neither (4) nor (5) can hold. In this case a group N conforms with the requirements of Theorem 1.1 if and only if N has an automorphism θ and an element $k = k_{11}$ so that $n\theta^2 = knk^{-1}$ for all $n \in N$ and $k\theta \neq k$. Thus, one is deprived of the selection $\theta = I$, which was so conveniently available in the proof of Corollary 1.4, and it is not very difficult to see that θ cannot even be an inner automorphism of N. If N is any Abelian group of exponent different from 2, one can choose $k \in N$ so that $k^2 \neq 1$ (i.e., $k \neq k^{-1}$) and let θ be defined by $n\theta = n^{-1}$ for all $n \in N$. There also exist acceptable groups N which are not Abelian. Using a computer, Professor J.G.F. Belinfante has determined that the smallest such groups which are not Abelian have order 16 and that there are two such groups of order 16. These two groups of order 16 can be identified as the smallest members of two well-known infinite families which are now described: (1) The dicyclic group of order $4n$ with $n > 0$ and divisible by 4 has generators a and b and relations $a^4 = b^{2n} = 1$, $ba = ab^{-1}$, $a^2 = b^n$. If one defines θ by $a\theta = ab$ and $b\theta = b^{n-1}$ and chooses $k = b^{n/2}$, then one sees that θ^2 is conjugation by $b^{n/2}$ and $k\theta = a^2b^{n/2} \neq k$. (2) Consider now those groups of order $2n$ where $n > 4$ is divisible by 4 which are generated by elements a and b subject to the relations $a^2 = b^n = 1$ and $ba = ab^{n/2+1}$. For such groups define θ by $a\theta = a$ and $b\theta = b^{n/2-1}$ and choose $k = b^2$. Then θ is an automorphism, θ^2 is conjugation by k, and $k\theta \neq k$.

Before leaving the present section it is tempting to formulate a generalization of Theorem 1.1 which would include non-prime cyclic extensions. A little work reveals that for such a generalization conditions (1), (2), and (3) remain intact while conditions (4), (5), and (6) must be replaced by ones which are considerably more complicated. The authors have not pursued this line of investigation because of its lack of relevancy in the context of G-loops.

2. Applications to G-loops

Recall that a loop L is called a G-loop provided that L is isomorphic to all of its loop isotopes. Any finite loop of order $n < 5$ is a group and, as such, is automatically a G-loop. R.L. Wilson [11(a), (b), (c)] proved that every finite G-loop of prime order is necessarily a group; he also constructed for each even integer $n > 5$ a G-loop of order n which is not a group. An intriguing question is the following: For each composite integer $n > 5$ does there exist a G-loop of order n which is not associative? The authors [5] have recently produced examples of G-loops of many composite orders and their constructions stem from the observation that any loop L for which

$$xy \cdot f = (xf) \cdot (yf)L(f)^{-1} \tag{9}$$

and

$$g \cdot xy = (gx)R(g)^{-1} \cdot (gy) \tag{10}$$

hold for all $x, y, f, g \in L$ must be a G-loop. It is, therefore, natural to see whether or not any loops of the type considered in §1 can satisfy (9) and (10).

THEOREM 2.1: *Let N be a group and let p be a prime. Then there exists a loop L so that N is the nucleus of L, N is normal in L, L/N is a group of order p, and L satisfies* (9) *and* (10) *for all $x, y, f, g \in L$ if and only if N has an automorphism θ and elements k_{ij} which satisfy the conditions set forth in Theorem* 1.1 *and also satisfy*

$$(k_{jl}k_{lj}^{-1})\theta^i \cdot k_{il}k_{i+l,j} = k_{ij}k_{i+j,l} \tag{11}$$

and

$$k_{ij}k_{ji}^{-1} \cdot k_{il}\theta^j \cdot k_{j,i+l} = k_{jl}\theta^i \cdot k_{i,j+l} \tag{12}$$

for all integers i, j, l with $1 \leq i, j, l \leq p-1$ (with the tacit understanding that subscripts in (11) *and* (12) *are to be reduced or interpreted modulo p whenever necessary and that $k_{0j} = k_{i0} = 1$).*

PROOF: With Theorem 1.1 available one needs only to show that (9) and (10) give rise to (11) and (12), and, conversely, that (11) and (12) imply (9) and (10). Actually (9) holds for all $x, y, f \in L$ if and only if the system of equations in (11) is satisfied, and a similar result links (10) and (12). Adopting the notation used in the proof of Theorem 1.1 and noting that (9) is trivially satisfied whenever any of x, y, f is 1, let $x = n_1 a^i$, $y = n_2 a^j$, and $f = n_3 a^l$ with none of i, j, l equal to 0. There are several cases which need to be considered by the reader. The details associated with one case will serve to illustrate what can be done routinely in all cases. For this purpose let $i + j < p$ and $i + l \geq p$. Then, keeping in mind that k_{ij} is central, one sees that

$$\begin{aligned} xy \cdot f &= (n_1 \cdot n_2\theta^i \cdot k_{ij} \cdot a^{i+j}) \cdot (n_3 a^l) \\ &= n_1 \cdot n_2\theta^i \cdot k_{ij} \cdot n_3\theta^{i+j} \cdot k_{i+j,l} a^{i+j+l-p} \\ &= n_1 \cdot n_2\theta^i \cdot n_3\theta^{i+j} \cdot k_{ij} \cdot k_{i+j,l} a^{i+j+l-p}. \end{aligned}$$

On the other hand, one has

$$\begin{aligned} (xf) \cdot (yf)L(f)^{-1} &= (n_1 \cdot n_3\theta^i \cdot k_{il} \cdot a^{i+l-p})(n_3^{-1} \cdot n_2 \cdot n_3\theta^j \cdot k_{jl}k_{lj}^{-1})\theta^{-l} \cdot a^j \\ &= n_1 \cdot n_3\theta^i \cdot k_{il}(n_3^{-1} \cdot n_2 \cdot n_3\theta^j \cdot k_{jl}k_{lj}^{-1})\theta^{i-p} \cdot k_{i+l-p,j} \cdot a^{i+j+l-p}. \end{aligned}$$

But note that

$$x\theta^{i-p} = y \Leftrightarrow k_{il} y k_{il}^{-1} = y\theta^p = x\theta^i \Leftrightarrow y = k_{il}^{-1} \cdot x\theta^i \cdot k_{il}.$$

Thus, the expression above for $(xf) \cdot (yf)L(f)^{-1}$ becomes

$$\begin{aligned} &n_1 \cdot n_3\theta^i(n_3^{-1} \cdot n_2 \cdot n_3\theta^j \cdot k_{jl}k_l^{-1})\theta^i \cdot k_{il}k_{i+l-p,j} a^{i+j+l-p} \\ &= n_1 \cdot n_2\theta^i \cdot n_3\theta^{i+j}(k_{jl}k_{lj})^{-1}\theta^i \cdot k_{il}k_{i+l-p,j} a^{i+j+l-p} \end{aligned}$$

and (11) follows.

With the other cases dealt with in similar fashion Theorem 2.1 is proved.

The G-loops of even order constructed by R.L. Wilson [11(a), (c)] are actually G-loops because of the following.

COROLLARY 2.2: *Any loop with index* 2 *nucleus is a* G-*loop*[3].

PROOF: Let L be a loop such that $[L:N] = 2$ where N denotes the nucleus of L. It is easy to see that $[L:N] = 2$ implies that N is normal

[3] This result has already appeared in the literature (see, for instance, V.D. Belousov [1]). What is of interest here is that this result can, in fact, be viewed as an immediate consequence of Theorem 2.1.

in L and that L/N is a group of order $p = 2$. There is only one k_{ij}, namely, $k_{1,p-l} = k_{11}$ and (11) and (12) are satisfied for any θ. Thus, by Theorem 2.1, L satisfies (9) and (10), so L is a G-loop.

In view of R.L. Wilson's concern (see [11(a), (c)]) about the possible existence of finite G-loops of orders divisible by 3 which are not groups, the following result is of interest.

COROLLARY 2.3: *There exists a G-loop having a normal nucleus of index* 3 *if there exists a group N with three elements k_{12}, k_{21}, and k_{22}, not all equal, and an automorphism θ such that*

(i) $n\theta^3 = k_{12}nk_{12}^{-1} = k_{21}nk_{21}^{-1} = k_{22}nk_{22}^{-1}$,

(ii) $k_{12}k_{21}^{-1}k_{22} = k_{21}\theta$,

(iii) $k_{12}k_{21}^{-1}k_{12}\theta^2 = k_{22}$,

(iv) $k_{22}\theta = k_{22}$

for all $n \in N$.

PROOF: Note that (11) holds for all i, j, l with $1 \le i, j, l \le p-1$ if and only if (11) holds, more specifically, for all i, j, l so that $1 \le j \le l \le p-1$. (Clearly (11) is trivially true whenever $j = l$ and the validity of equations (11) with $j > l$ is an immediate consequence of their validity with $j < l$.) In other words, one need only be concerned with system (11) in the case $j < l$. Similar observations indicate that only the case $i < j$ is relevant when examining system (12). Taking advantage of this reduction and taking $p = 3$, one sees that systems (11) and (12) are equivalent to

$$(k_{12}k_{21}^{-1})\theta \cdot k_{12} = k_{22},$$

$$(k_{12}k_{21}^{-1})\theta^2 \cdot k_{22} = k_{21},$$

$$k_{12} \cdot k_{21}^{-1} \cdot k_{22} = k_{21}\theta,$$

$$k_{12}k_{21}^{-1} \cdot k_{12}\theta^2 = k_{22}\theta.$$

Applying θ to the last equation, using the first equation to substitute for $(k_{12}k_{21}^{-1})\theta$, and noting that $k_{12}\theta^3 = k_{12}$, one obtains $k_{22}\theta^2 = k_{22}$. Applying θ to both sides of this last expression, one sees that k_{22} is fixed by θ. Thus, in the presence of (i), systems (11) and (12) are equivalent to (ii), (iii), and (iv). Thus, using Theorems 1.1 and 2.1, one obtains a loop L having N as nucleus of index 3 and satisfying (9) and (10) for all x, y, f, $g \in L$. Since L satisfies (9) and (10), the loop L is a G-loop, and the proof is complete.

It is not difficult to find groups which do meet the requirements set forth for N in the preceding corollary. Let q be any prime such that $q \equiv 1 \pmod 3$, let (q) denote the principal ideal generated by q in the ring Z of integers, and for each $m \in Z$ let $\bar{m}$ denote the additive coset $\bar{m} = m + (q)$ in the ring $Z/(q)$. Now let N be the additive group of the ring $Z/(q)$. Since $q \equiv 1 \pmod 3$, it follows from elementary number theory that there is an integer s so that $s^3 \equiv 1 \pmod q$ and $s \not\equiv 1 \pmod q$. Define $\bar{a}\theta = \overline{sa}$ for all $\bar{a} \in N$ and note that θ is an automorphism of N. Now select $k_{22} = \bar{0}$, $k_{21} = \bar{1}$, and $k_{12} = \overline{1+s}$. The conditions of Corollary 2.3 hold for N and so there does exist a G-loop L of order $3q$ which is not a group. It might be interesting to see what L actually looks like. Returning to the proof of Theorem 1.1 and adopting a notation consistent with the present discussion, it is clear that L is the Cartesian product $Z/(q) \times Z/(3)$ with a binary operation for L defined by

$$(\bar{a},\ \bar{i})(\bar{b},\ \bar{j}) = (\overline{a + sb} + k_{ij},\ \overline{i+j}),$$

which is merely expression (7) rewritten. Since the ordinary direct product of G-loops is a G-loop (see R.L. Wilson [11(a)] and since all groups are G-loops, one can use the loop L constructed above to obtain the following result: *For each positive integer m which has at least one prime divisor q with* $q \equiv 1 \pmod 3$, *there exists a G-loop of order* $3m$ *which is not a group.*

For primes $p > 3$ systems (11) and (12) are much more complicated even though the reduction mentioned at the start of the proof of Corollary 2.3 is still available. Setting $i = 1$ and keeping j and l arbitrary, but subject to the restraints $j < p-1$ and $j + l < p - 1$, one obtains from (12) that $k_{j,l+1} = k_{j1} \cdot k_{jl}\theta$ from which it follows that

$$k_{jr} = k_{j1} \cdot k_{j1}\theta \cdot k_{j1}\theta^2 \cdots k_{j1}\theta^{r-l} \tag{13}$$

for all r such that $0 < r \leq p - j - 1$. Again with $i = 1$ and $j < p - 1$, but now with $j + l \geq p - 1$, one obtains from (12) in similar fashion that

$$k_{jr} = k_{j1} \cdot k_{j1}\theta \cdot k_{j1}\theta^2 \cdots k_{j1}\theta^{r-l} \cdot k_{1,p-1}\theta^{j+r-p} \tag{14}$$

for all r with $r \geq p - j$. Now, examining (12) with $i = 1$, $j = p - 1$, and $l < p - 1$, one obtains $k_{1,p-1} \cdot k_{p-1,1}^{-1} \cdot k_{p-1,l+1} = k_{p-1,l}\theta \cdot k_{1,p-1+l} = k_{p-1,l}\theta$ (with the understanding always that subscripts are to be reduced modulo p);

so with $k = k_{1,p-1} \cdot k_{p-1,1}^{-1}$ one has

$$(15) \qquad k_{p-1,r} = k \cdot k\theta \cdot k\theta^2 \cdots k\theta^{r-2} \cdot k_{p-1,1}\theta^{r-1}$$

for all r such that $r \leq p-1$.

Setting $i = l = 1$ and keeping $j < p-1$ in (11), one obtains

$$(16) \qquad k_{j1}\theta \cdot k_{2j} = k_{j+1,1}.$$

But $k_{2j} = k_{21} \cdot k_{21}\theta \cdot k_{21}\theta^2 \cdots k_{21}\theta^{j-1}$ if $j \leq p-3$ because of (13). Hence, one obtains from (16) that

$$(17) \qquad k_{j1} = k_{21} \cdot k_{21}^2\theta \cdot k_{21}^3\theta^2 \cdots k_{21}^{j-1}\theta^{j-2}$$

for all j such that $j \leq p-2$. Since $p > 3$ one sees from condition (2) of Theorem 1.1 that k_{21} is a central element of N. Consequently, setting $i = j = 1$ and $l = p-2$ in (11) and using (17), one obtains

$$\begin{aligned} k_{2,p-2} &= k_{p-2,1}^{-1}\theta \cdot k_{p-1,1} \\ &= k_{21}^{-1}\theta \cdot k_{21}^{-2}\theta^2 \cdots k_{21}^{-(p-3)}\theta^{p-3} \cdot k_{1,p-1}. \end{aligned}$$

Comparing this expression for $k_{2,p-2}$ with the one which can be obtained from (14), one sees that

$$(18) \qquad k_{p-1,1}k_{1,p-1}^{-1} = k_{21} \cdot k_{21}^2\theta \cdot k_{21}^3\theta^2 \cdots k_{21}^{p-2}\theta^{p-3}.$$

Now set $i = 1$, $j = 2$, and $l = p-1$ in (12) and use (14) to get

$$\begin{aligned} k_{21}^{-1} \cdot k_{1,p-1}\theta^2 &= k_{2,p-1}\theta \\ &= k_{21}\theta \cdot k_{21}\theta^2 \cdots k_{21}\theta^{p-l} \cdot k_{1,p-1}\theta^2. \end{aligned}$$

Thus, an important relationship has been discovered, namely,

$$(19) \qquad k_{21} \cdot k_{21}\theta \cdot k_{21}\theta^2 \cdots k_{21}\theta^{p-l} = 1.$$

Now let $j = 1$, $l = 3$, and $i = p-3$ in (11) to get

$$(20) \qquad k_{31}^{-1}\theta^{p-3} \cdot k_{p-3,3} = k_{p-3,1} \cdot k_{p-2,3}.$$

In view of (14) one can replace $k_{p-3,3}$ in (20) by $k_{p-3,1} \cdot k_{p-3,1}\theta \cdot k_{p-3,1}\theta^2 \cdot k_{1,p-1}$. Making this replacement and noting that $k_{p-3,1}$ is a central element of N, one has

$$(21)\qquad k_{31}^{-1}\theta^{p-3}\cdot k_{p-3,1}\theta\cdot k_{p-3,1}\theta^{2}\cdot k_{1,p-1}=k_{p-2,3}=k_{p-2,1}\cdot k_{p-2,2}\theta$$

where the last equality can be justified by setting $i=1$, $j=p-2$, and $l=2$ in (12). Now with $j=1$, $l=2$, and $i<p-3$ in (11) and with k_{i1} and $k_{i+2,1}$ computed by (17) one obtains $k_{i+1,2}=k_{21}^{i}\theta^{i-1}\cdot k_{21}^{i}\theta^{i}\cdot k_{i2}$ and so it follows that

$$k_{p-3,2}=k_{21}\cdot k_{21}^{3}\theta\cdot k_{21}^{5}\theta^{2}\cdots k_{21}^{2(p-3)-3}\theta^{p-5}\cdot k_{21}^{p-4}\theta^{p-4}.$$

Setting $j=1$, $l=2$, and $i=p-3$ in (11), using the above expression for $k_{p-3,2}$, and employing an expression for $k_{p-3,1}$ obtainable from (17), one obtains

$$\begin{aligned}k_{p-2,2}&=k_{p-3,1}^{-1}\cdot k_{21}^{-1}\theta^{p-3}\cdot k_{p-3,2}\cdot k_{p-1,1}\\&=k_{21}\theta\cdot k_{21}^{2}\theta^{2}\cdot k_{21}^{3}\theta^{3}\cdots k_{21}^{p-4}\theta^{p-4}\cdot k_{21}^{-1}\theta^{p-3}\cdot k_{p-1,1}.\end{aligned}$$

It now follows directly from (21) that

$$(22)\qquad k_{p-1,1}\theta\cdot k_{1,p-1}^{-1}=k_{21}\theta^{p-1}.$$

It should be noted at this point that, if N is a group with an automorphism θ and elements $k_{1,p-1}$, $k_{p-1,1}$, and k_{21} satisfying (18), (19), and (22), then the set of k_{ij}'s defined by (13), (14), and (15) provide a common solution to systems (11) and (12). Consequently, if p is a prime with $p>3$, one gets a corollary analogous to Corollary 2.3. Specifically, one can establish

COROLLARY 2.4: *Let p be a prime with $p>3$. Then there is a G-loop having a normal nucleus of index p if there exists a group N, elements $k_{1,p-1}$, $k_{p-1,1}$, $k_{21}\in N$ (k_{21} central), and an automorphism θ such that $n\theta=k_{1,p-1}nk_{1,p-1}^{-1}=k_{p-1,1}nk_{p-1,1}^{-1}$ for all $n\in N$ and such that* (18), (19), *and* (20) *hold.*

Let p be any prime with $p>5$. Now let q be any prime such that $q\equiv 1 \pmod p$ and note that there must exist an integer s so that $s^{p}\equiv 1$ (mod q) and $s\not\equiv 1$ (mod q). Using the notation and strategy from the discussion immediately following the proof of Corollary 2.3, one chooses N to be the additive group of the ring $Z/(q)$. Just as before, define θ by $\bar{a}\theta=\overline{sa}$ for all $\bar{a}\in N$. Then θ is an automorphism of N.

Since

$$s^{p-1}+s^{p-2}+\cdots+s+1\equiv 0 \pmod{q},$$

it is clear that k_{21} can be selected to be any element in N and (19) will be satisfied. Suppose that one can find an element $k_{1,p-1}$ in N satisfying

$$k_{1,p-1}+k_{1,p-1}^{-1}\theta = k_{21}+k_{21}^{2}\theta+k_{21}^{3}\theta^{2}+\cdots+k_{21}^{p-1}\theta^{p-2}. \tag{23}$$

If one then selects $k_{p-1,1}$ by

$$k_{p-1,1}=(k_{21}\theta^{p-1}+k_{1,p-1})\theta^{-1},$$

it is easy to see that (18) and (22) also hold. Thus, one will meet with success, if one can select an element $k_{1,p-1}$ in N so that (23) holds. But note that (23) has a solution of the form

$$k_{1,p-1}=\bar{a}_0+\overline{sa_1}+\bar{s}^2\bar{a}_2+\cdots+\bar{s}^{p-2}\bar{a}_{p-2}$$

if and only if $a_0, a_1,\ldots, a_{p-2}$ are integers so that

$$\tag{24} \begin{cases} a_0+a_{p-2} & \equiv 1,\\ a_1-a_0+a_{p-2} & \equiv 2,\\ a_2-a_1+a_{p-3} & \equiv 3,\\ \quad\vdots & \\ a_{p-3}-a_{p-4}+a_{p-2} & \equiv p-2,\\ 2a_{p-2}-a_{p-3} & \equiv p-1 \pmod{q}. \end{cases}$$

Adding, one easily deduces from (24) that

$$pa_{p-2}\equiv \tfrac{1}{2}p(p-1) \pmod{q}.$$

The assumption that $q\equiv 1 \pmod{p}$ guarantees that $p\not\equiv 0 \pmod{q}$ and, hence, $a_{p-2}\equiv \frac{1}{2}(p-1) \pmod{q}$. Having obtained a_{p-2}, one can return to (24) and, in succession, obtain $a_{p-3}, a_{p-4},\ldots, a_0$. Consequently, the group N satisfies the conditions of Corollary 2.4. Then, just as in an earlier argument, one is now in a position to make the following assertion: *If p is a prime with $p>5$ and if m is any positive integer with at least one prime divisor q such that $q\equiv 1 \pmod{p}$, then there exists a G-loop of order pm which is not a group.*

The authors conclude this paper with a corollary which serves as a word of practical advice to those readers who may wish to exploit Theorem 2.1 to obtain additional examples of G-loops.

COROLLARY 2.5: *Let p be a prime with $p > 3$ and let N be a finite group with an automorphism θ and elements k_{ij} satisfying the conditions of Theorem 2.1. If p does not divide the order of N, then necessarily θ cannot be the identity automorphism of N.*

PROOF: Suppose that $\theta = I$. Then it follows from (19) that $k_{21}^p = 1$. But with $p \nmid |N|$ one must then conclude that $k_{21} = 1$. It follows from (17) that $k_{j1} = 1$ for $j < p - 1$; it follows from (13) that $k_{jr} = 1$ for $j + r < p$; it follows from (14) that $k_{jr} = k_{1,p-1}$ for $j + r \geq p$ and $j < p - 1$. Consulting (18), one sees that $k_{p-1,1} = k_{1,p-1}$ and so it follows that $k_{p-1,r} = k_{p-1,1}$. Thus, none of (4), (5), and (6) holds and a contradiction is reached.

REFERENCES

[1] V.D. BELOUSOV: *Foundations of the theory of quasigroups and loops* (Russian), Izdat. "Nauka", Moskow, 1967.

[2] R.H. BRUCK: *A survey of binary systems*, Springer-Verlag, 1958.

[3] R.P. BURN: Finite Bol loops, *Math. Proc. Cambridge Philos. Soc.* 84 (1978), no 3, 377–385.

[4] ORIN CHEIN: Moufang loops of small order I., *Trans. Amer. Math. Soc.* 188 (1974) 31–51.

[5] EDGAR G. GOODAIRE and D. A. ROBINSON: A class of loops which are isomorphic to all loop isotopes, submitted.

[6] MARSHALL HALL, Jr.: *The theory of groups*, Macmillan, 1959.

[7] HARALD NIEDERREITER and KARL H. ROBINSON: Bol loops of order pq, to appear.

[8] J. MARSHALL OSBORN: Loops with the weak inverse property, *Pacific J. Math.* 10 (1960) 295–304.

[9] D.A. ROBINSON: Bol loops, *Trans. Amer. Math. Soc.* 123 (1966) 341–354.

[10] ERIC L. WILSON: A class of loops with the isotopy–isomorphy property, *Canad. J. Math.* 18 (1966) 589–592.

[11] ROBERT L. WILSON, Jr.: (a) Loop isotopism and isomorphism and extensions of universal algebras, Ph.D. Thesis, University of Wisconsin, Madison, 1969. (b) Isotopy–isomorphy loops of prime order, *J. Algebra* 31 (1974) 117–119. (c) Quasidirect products of quasigroups, *Comm. Algebra* 3(9) (1975) 835–850.

(Oblatum 30-V-1980 & 3-IV-1980)

Department of Mathematics
and Statistics
Memorial University of Newfoundland
St. John's Newfoundland
Canada A1B 3X7

School of Mathematics
Georgia Institute of Technology
Atlanta, Georgia 30332
U.S.A.