NILPOTENCY CONDITIONS FOR FINITE LOOPS

BY
C. R. B. WRIGHT

Introduction

The purpose of this note is to consider various properties of loops which are related to central nilpotency, and to determine some of the implications which hold among them. Since some of the properties considered are equivalent to nilpotency for the class of finite groups, it is natural to ask whether or not any of the properties is equivalent to central nilpotency for an interesting class of finite loops. Another reason for studying the problem is that the standard, group-theoretic proofs in the area of nilpotency ultimately depend on the rather remarkable properties of Sylow normalizers. Since neither "Sylow subloops" nor normalizers exist, in general, for loops, some of the proofs and counterexamples obtained for loops expose the essential reasons behind the success of the theory for groups.

The paper is divided as follows. In Section 1 we present the conditions to be studied and list some of the implications among them which hold for loops in general. Various pathological examples lead us to restrict ourselves to power-associative loops. We begin Section 2 with a general theorem about power-associative loops. Although the result is not deep, it seems to be new, perhaps because no one needed it before. Using this theorem, we next give a method for constructing new, power-associative loops from old ones. In particular, we construct enough pathological examples to show that the results for power-associative loops must be meager. In Section 3, therefore, we consider diassociative loops. We are able to show that some reasonably interesting implications hold for rather restricted classes of diassociative loops, and we obtain an example which shows that even commutative, diassociative 2-loops are ill-mannered, indeed. In the final section, we touch briefly on the problem for Moufang loops and note that a certain amount of pathology is still present.

1. The problem for general loops

Throughout what follows we use the notation of [1]. In addition, the symbol $\langle A \rangle$ stands for the subloop generated by the set A, and $| A |$ is the order of $\langle A \rangle$. We use the symbol $A \leq B$ ($A < B$) to stand for the statement that A is a subloop of B (and is not B) and use $A \lhd B$ to mean that A is a normal subloop of B. We parallel the definition in Kurosh [5, p. 215] and define an N-loop to be a loop in which every proper subloop is normal in a strictly larger subloop. Finally, if π is a set of primes, we let π' be the complementary set and call a loop a π-loop in case it is power-associative and con-

Received January 18, 1964.

tains no element of infinite order or of order a prime in π'. We call a $\{p\}$-loop a p-loop.

Let G be a loop. The conditions on G which we wish to consider are:

(1) G is centrally nilpotent;
(2) G is an N-loop;
(3) G is a direct sum of p-loops;
(4) G is commutative;
(5) G is Hamiltonian.

It is well known that if G is a finite group, then (1), (2) and (3) are equivalent and are implied by each of (4) and (5). When any of these conditions holds for a finite group, G, then also

(6) every non-trivial maximal subloop of G has a non-trivial center which is normal in G,

so that

(6′) every non-trivial maximal subloop of G contains a non-trivial G-normal subloop in its center.

It was essentially observed by Bruck [2, p. 275] that (1) implies (2) for arbitrary loops. Clearly, (5) implies (2), and since (1) is inherited by subloops and factor loops, (1) and (5) together imply (6). In the negative direction, it is possible to construct a commutative loop of order 7 with no proper subloops and, by extending this loop by a group of order 3, to produce a loop of order 21 which is commutative and Hamiltonian but does not satisfy (1), (3) or (6′).

In what follows we shall produce examples which show that, except as just noted, no one of (1), $\cdots$, (5) implies any other. In view of the existence of such examples, it seems essential to place some restriction on the loops considered in order to relate arithmetical, normal and central properties.

2. A kite-tail construction for power-associative loops

The purpose of this section is to exhibit a method of extending a cyclic group by a power-associative loop in such a fashion that the extension is a power-associative loop. We begin with a result about generators of power-associative loops. In the statement and proof of the theorem we use the notation x to stand for $\langle x \rangle$ where there can be no ambiguity and write $H:K$ for the index of K in H.

THEOREM 1. *Let G be a power-associative loop. Then G contains a subset, B, with the properties that*

(i) *for each x in G there is a y in B with $\langle x \rangle = \langle y \rangle$, and*

(ii) *if y and z are in B with $y \cap z \neq 1$ and with $y:y \cap z = a$ and $z:y \cap z = b$, then $y^a = z^b$.*

Proof. Let $\mathfrak{B}$ be the collection of all subsets, B, of G satisfying (ii), and partially order $\mathfrak{B}$ by inclusion. Since $\mathfrak{B}$ has finite character, by Tukey's Lemma $\mathfrak{B}$ has a maximal member, say B_0. We show that B_0 satisfies (i) by considering cases. Let x be in G.

Case 1. $|x|$ is a power of a prime, p. Choose y in B_0 so that $x{:}x \cap y$ is minimal, say $x{:}x \cap y = a$ and $y{:}x \cap y = b$. Since $x \cap y = \langle x^a \rangle = \langle y^b \rangle$, there is an integer, n, such that $y^b = x^{an}$. Let $u = x^n$. Since n is prime to p, $\langle u \rangle = \langle x \rangle$. Suppose that z is in B_0 and that $u{:}u \cap z = c$ and $z{:}u \cap z = d$. Since $x{:}x \cap y$ is minimal, and since $\langle x \rangle$ is a cyclic p-group, $u \cap z \leq u \cap y$. Hence, $u \cap z = u \cap z \cap y \leq z \cap y$. If $y{:}z \cap y = e$ and $z{:}z \cap y = f$, then $y^e = z^f$, since y and z are in B_0. Let $g = z \cap y{:}u \cap z$ and $h = u \cap y{:}u \cap z$. Then $c = ah$, $d = fg$ and $y{:}u \cap z = eg = bh$. Hence,

$$u^c = u^{ah} = y^{bh} = y^{eg} = z^{fg} = z^d.$$

Since z was an arbitrary member of B_0, $B_0 \cup \{u\}$ satisfies (ii). Thus u is in B_0. We have shown that if $|x|$ is a prime-power, then there is a u in B_0 with $\langle x \rangle = \langle u \rangle$.

Case 2. $|x|$ is finite. In view of the result of Case 1, we may assume inductively that $\langle x \rangle = \langle y \rangle \langle z \rangle$ with y and z in B_0 and with $y \cap z = 1$. If $|y| = b$ and $|z| = a$, then $x{:}x \cap y = a$, $x{:}x \cap z = b$, and $|x| = ab$. There are integers, n and m, such that $an + bm = 1$. Let $u = y^n z^m$. Then $u^a = y$, $u^b = z$, and $\langle x \rangle = \langle u \rangle$. Suppose that w is in B_0 and that $x{:}x \cap w = e$, $w{:}x \cap w = f$, $y{:}y \cap w = g$, $w{:}y \cap w = hf$, $z{:}z \cap w = i$ and $w{:}z \cap w = jf$. Now

$$x \cap w = (y \cap w) \oplus (z \cap w), \qquad x \cap w{:}y \cap w = h, \qquad x \cap w{:}z \cap w = j,$$

so that $|z \cap w| = h$ and $|y \cap w| = j$. Hence,

$$hi = |z \cap w| \cdot (z{:}z \cap w) = |z| = a,$$

and similarly $gj = b$. Thus,

$$gihj = ba = |x| = e \cdot |x \cap w| = ehj,$$

so that $gi = e$. Moreover, since y, z and w are in B_0, $y^g = w^{hf}$ and $z^i = w^{jf}$. Hence,

$$u^e = u^{gi} = y^{gin} z^{gim} = w^{hfin+jfgm} = w^{anf+bmf} = w^f.$$

Since w was an arbitrary member of B_0, $B_0 \cup \{u\}$ satisfies (ii), and u is in B_0. The proof of Case 2 is completed by induction on $|x|$. Thus if $|x|$ is finite, there is a u in B_0 such that $\langle x \rangle = \langle u \rangle$.

Case 3. $|x|$ is infinite. There is a y in B_0 such that $x \cap y \neq 1$, since otherwise $B_0 \cup \{x\}$ would vacuously satisfy (ii). If $x{:}x \cap y = a$ and $y{:}x \cap y = b$, then $x^a = y^{nb}$, where $n = \pm 1$. Let $u = x^n$. Then $\langle u \rangle = \langle x \rangle$. If z is in B_0, and if $x{:}x \cap z = c$ and $z{:}x \cap z = d$, then $x^c = z^{md}$, where $m = \pm 1$. Now $1 \neq x^{ac} \in y \cap z$, so that $x \cap y \cap z \neq 1$. Let $x \cap y \cap z = w$. We have

$$(x{:}x \cap y)(y{:}y \cap z)(z{:}z \cap x)$$
$$= (x{:}w)(y{:}w)(z{:}w)/(x \cap y{:}w)(y \cap z{:}w)(z \cap x{:}w)$$
$$= (x{:}z \cap x)(y{:}x \cap y)(z{:}y \cap z),$$

so that $a(y{:}y \cap z)d = cb(z{:}y \cap z)$. Thus, since y and z are in B_0,

$$x^{a(y:y\cap z)d} = x^{cb(z:y\cap z)} = z^{mdb(z:y\cap z)} = y^{mdb(y:y\cap z)} = x^{mdna(y:y\cap z)}.$$

Hence, $mn = 1$ and $m = n$. Thus $u^c = z^d$. Since z was an arbitrary member of B_0, it follows, as above, that u is in B_0.

We have shown that for each x in G there is a u in B_0 such that $\langle x\rangle = \langle u\rangle$. Thus B_0 satisfies (i), and the theorem is proved.

Notice that if the orders of the elements of G are bounded, then by selecting those members of B_0 which generate maximal cyclic subgroups of G we get a subset, B_1, of G with the properties that

(i′) if x is in G, then there is a y in B_1 with x in $\langle y\rangle$,

(ii) if y and z are in B_1 with $y \cap z \neq 1$ and with $y{:}y \cap z = a$ and $z{:}y \cap z = b$, then $y^a = z^b$, and

(iii) if y and z are in B_1, then y is not in $\langle z\rangle$.

In view of the existence of groups of type p^∞, we cannot hope for such an independent, cyclic basis in an arbitrary torsion loop.

Let H be a power-associative loop. Let C be a cyclic group written additively. We construct an extension, G, of C by H as follows. For each ordered pair, (h, k), of elements of H which do not lie in a common cyclic subgroup of H, arbitrarily choose a quasi-group, $(C, *_{h,k})$, whose elements are those of C. Choose a subset, B, of H satisfying (i) and (ii) of Theorem 1. Let $G = C \times H$, and define multiplication in G as follows. If $\langle h, k\rangle$ is not cyclic, let

$$(a, h)(b, k) = (a *_{h,k} b, hk).$$

If h and k lie in $\langle g\rangle$ for some g in B, and if $h = g^m$ and $k = g^n$ (with $0 \leq m < |g|$ and $0 \leq n < |g|$ if $|g|$ is finite) define

$$(a, h)(b, k) = (a + b, hk) \qquad \text{if} \quad m + n < |g|$$

and

$$(a, h)(b, k) = (a + b + 1, hk) \quad \text{if} \quad m + n \geq |g|.$$

One can check that condition (ii) of Theorem 1 insures that the definition of multiplication in G is independent of the choice of g in B. It is not difficult to check also that G is a loop with $(0, 1)$ as identity. For each h in H, $C \times \langle h\rangle$ is a subloop of G. If $\langle h\rangle = \langle b\rangle$ with b in B and of finite order, then $C \times \langle h\rangle$ is a cyclic group generated by $(0, b)$. If $|h|$ is infinite, then

$$C \times \langle h\rangle = C \times \langle b\rangle \cong C \oplus \langle b\rangle.$$

In either event, (a, h) generates a cyclic group for each a i C and h in H; hence G is power-associative.

Notice that if H is a p-loop and C is of order p, then, since $C \times \langle 1 \rangle$ is contained in the cyclic p-group $\langle (a, h) \rangle$ for each non-trivial (a, h) in G, $C \times \langle 1 \rangle$ is contained in every proper subloop of G. Thus the lattice of (normal) subloops of G is the lattice of (normal) subloops of H with a segment attached at the bottom. Since G is also a p-loop, we may repeat the process and attach another segment to the bottom of the lattice of G. Continuing in this way, we can construct a p-loop whose lattice of subloops consists of the lattice of subloops of H with an arbitrarily long tail at the bottom.

We can use the construction just given to produce examples of pathological, power-associative loops. Norton [6] defines a Hamiltonian loop to be a loop in which every subloop is normal and proves that every non-abelian, power-associative, Hamiltonian loop is a direct sum of p-loops. We show now that if p is odd, then a commutative, Hamiltonian p-loop need not be centrally nilpotent. Hence, (3), (4) and (5) are together insufficient to imply central nilpotency.

Let H be a Hamiltonian p-loop—for example, a non-cyclic group of order p^2—and let C be cyclic of order p. In view of the remarks above, $C \times \langle 1 \rangle$ is the unique minimal subloop of G, and G is a Hamiltonian p-loop. Routine calculation shows that $C \times \langle 1 \rangle$ is in the center of G if, and only if,

$$a *_{h,k} b = (0 *_{h,k} 0) + a + b$$

for every a and b in C whenever $\langle h, k \rangle$ is non-cyclic. If p is odd and H is non-cyclic, then for each ordered pair, (h, k), in $H \times H$ for which $\langle h, k \rangle$ is non-cyclic we can choose $*_{h,k}$ in such a way that $a *_{h,k} b = b *_{h,k} a$ (so that G is commutative if H is) but so that $a *_{h,k} b$ is not given by $(0 *_{h,k} 0) + a + b$. For example, if we agree on a particular order for $\{h, k\}$, we can define

$$a *_{h,k} b = a - b = b *_{h,k} a.$$

Thus G can be a commutative, Hamiltonian p-loop with trivial center.

It is easy to see that a finite, Hamiltonian 2-loop is necessarily centrally nilpotent. However, if we begin with the Klein 4-group for H and iterate the extension process n times we can obtain a commutative, Hamiltonian 2-loop of order 2^{n+2} which is nilpotent of class $n + 1$, the highest class a loop of this order can have.

The construction given can also be used to produce nilpotent, power-associative loops which are not direct sums of p-loops. For example, letting H be the Klein 4-group and C be of order 3, we can require that $C \times \langle 1 \rangle$ be in the center of G but that G be non-commutative, or we can require that $C \times \langle 1 \rangle$ be in the center of G, that G be commutative, and that G have no normal 2-subloops.

3. The diassociative case

The following theorem shows that the normal structure of a diassociative loop has a bearing on the arithmetical properties of the loop.

THEOREM 2. *If G is a locally finite, diassociative N-loop then G is a direct sum of p-loops for various primes, p.*

Proof. Let π be a set of primes. If A is a power-associative loop, let A_π be the set of all elements of A whose orders are products of powers of primes in π. If H is a finitely generated subgroup of G, then H is a finite N-group, so that H is nilpotent, and $H = H_\pi \oplus H_{\pi'}$. If x and y are in G_π, then $\langle x, y\rangle = \langle x, y\rangle_\pi \oplus \langle x, y\rangle_{\pi'}$, so that $\langle x, y\rangle = \langle x, y\rangle_\pi$, since x and y are in $\langle x, y\rangle_\pi$. Thus xy and x^{-1} are in G_π. It follows that G_π (and similarly, $G_{\pi'}$) is a subloop of G. If z is in G, then $\langle z\rangle = \langle z\rangle_\pi \oplus \langle z\rangle_{\pi'}$; hence, $G = G_\pi \cdot G_{\pi'}$. If a and b are in G_π and if x and y are in $G_{\pi'}$, then

$$\langle ax\rangle = \langle a\rangle \oplus \langle x\rangle \quad \text{and} \quad \langle by\rangle = \langle b\rangle \oplus \langle y\rangle,$$

so that

$$\langle ax, by\rangle = \langle a, x, b, y\rangle = \langle a, b\rangle \oplus \langle x, y\rangle.$$

Hence, $ax \cdot by = ab \cdot xy$. Since the mapping $ax \to a \oplus x$ is an isomorphism of G onto $G_\pi \oplus G_{\pi'}$, it follows that $G = G_\pi \oplus G_{\pi'}$. Letting π consist of one prime at a time, we conclude that G is a direct sum of p-loops.

COROLLARY. *A locally finite, centrally nilpotent, diassociative loop is a direct sum of p-loops.*

Later in this section we shall give an example of a finite, commutative, diassociative N-loop which is also a 2-loop but which is not nilpotent. In the light of this example, it seems reasonable to examine conditions other than (3) and (4) which, in conjunction with (2), will insure nilpotency of a finite, diassociative loop. We begin with a technical lemma suitable for use with induction on the order of a loop.

Let G_n denote the n-th member of the lower central series of G.

LEMMA 3. *Let G be a loop such that*

(i) $G_n = G_{n+1} > 1$ *for some positive integer n,*
(ii) *G satisfies the maximal condition for subloops,*
(iii) *if $1 < H \lhd G$, then G/H is centrally nilpotent, and*
(iv) *G satisfies (6′).*

Then G can be generated by two elements.

Proof. Suppose that $1 < H \lhd G$. Then

$$(G/H)_n = G_n H/H = G_{n+1} H/H = (G/H)_{n+1},$$

so that by (iii), $G_n \leq H$. If $\langle 1\rangle$ is a maximal subloop of G, then G can be generated by one element. Suppose that $\langle 1\rangle$ is not maximal. According to (ii), G has maximal subloops, and according to (iv), each contains a non-trivial, G-normal subloop in its center. Hence, $G_n \leq Z(M)$ for each maximal subloop, M, of G, so that $G_n \leq \Phi(G) < G$, where $\Phi(G)$ is the Frattini subloop of G. Let u be in G_n and $u \neq 1$. Since $u \notin Z(G)$, there exist x and y in G

such that $u \notin Z(\langle x, y, u\rangle)$. If $\langle x, y, u\rangle \leq M$ with M maximal in G, then $u \notin Z(M)$, a contradiction. Thus $\langle x, y, u\rangle = G$. Since $u \in \Phi(G)$, $\langle x, y\rangle = G$.

Remark. Condition (i) of Lemma 3 certainly holds in case G is finite but not nilpotent. One can also show that Lemma 3 remains true if (i) is replaced by

(i′) G/G' is finite and G is not nilpotent.

THEOREM 4. *If G is a finite, diassociative loop in which*

(7) *every maximal subloop is normal,*

and if G, together with all of its homomorphic images, satisfies (6′), *then G is centrally nilpotent.*

Proof. Suppose that G is a counterexample of minimal order. Since every maximal subloop of G is normal, G is not a group; hence, G is not generated by two elements. Since G satisfies (i), (ii) and (iv) of the lemma, G has a proper, normal subloop, H, such that G/H is not centrally nilpotent. But then G/H is a smaller counterexample than G. Hence, G does not exist, and the theorem is proved.

Bruck and Paige [4] define an A-loop to be a loop all of whose inner mappings are automorphisms.

THEOREM 5. *A finite, diassociative A-loop which is also an N-loop is centrally nilpotent.*

Proof. Let G be a minimal counterexample. Since G is an N-loop, G is not a group, so that G cannot be generated by two elements. Now G satisfies (i), (ii) and (iii) of Lemma 3, since according to [4] every homomorphic image of an A-loop is an A-loop. Moreover, every subloop of an A-loop is an A-loop. Thus, if M is maximal in G, then M is centrally nilpotent, so that $Z(M) > 1$. Since $M \lhd G$ and $Z(M)$ is characteristic in M, $Z(M) \lhd G$. Thus G satisfies (6) and hence also (6′), so that G is a counterexample to the lemma. We conclude that G does not exist.

In connection with these last two theorems, note that for finite groups condition (7), while not obviously inherited by subgroups, turns out to be equivalent to nilpotency and hence, to be hereditary. It is possible that (7) is equivalent to (2) for finite, diassociative loops. I have no examples to the contrary. On the other hand, in order to make the proofs work, I have had to assume either that condition (6′) on maximal subloops is inherited by factor loops or else that (2) holds, i.e., that every subloop has (7).

As a final step in the positive direction, we note that it follows from Norton's work that every diassociative, Hamiltonian loop is centrally nilpotent of class at most 2, so that (5) implies (1) for diassociative loops.

In the negative direction, now, it is not difficult to find a loop of order 10 in which every two elements generate a group of exponent 2. Such a loop

satisfies (3) and (4) but not (7), so that it fails to satisfy (1) or (2). With somewhat more trial and error one can even find a loop of order 16 and of exponent 2 in which Lagrange's Theorem is hereditary but in which there is a (non-normal) maximal subloop of order 4. Thus (3) and (4) have little to do with the subnormal structure of a diassociative loop. The following example shows that one can expect almost no justice at all when dealing with diassociative loops.

Let A be an elementary abelian group of order 4, generated by a and b, and let W be an elementary abelian group of order 8, generated by x, y and z. Let α, β and γ be the automorphisms of A such that $a\alpha = ab$, $(ab)\alpha = a$, $b\beta = ab$, $(ab)\beta = b$ and $\gamma = \alpha\beta\alpha$. Let $G = A \times W$ with multiplication defined as follows. For each c and d in A, let

$$\begin{aligned}
(c, x)(d, y) &= ((cd)\alpha, xy) &&= (d, y)(c, x)\\
(c, x)(d, xy) &= (c\cdot d\alpha, y) &&= (d, xy)(c, x)\\
(c, y)(d, xy) &= (c\cdot d\alpha, x) &&= (d, xy)(c, y)\\
\\
(c, x)(d, z) &= ((cd)\beta, xz) &&= (d, z)(c, x)\\
(c, x)(d, xz) &= (c\cdot d\beta, z) &&= (d, xz)(c, x)\\
(c, z)(d, xz) &= (c\cdot d\beta, x) &&= (d, xz)(c, z)\\
\\
(c, x)(d, yz) &= ((cd)\gamma, xyz) &&= (d, yz)(c, x)\\
(c, x)(d, xyz) &= (c\cdot d\gamma, yz) &&= (d, xyz)(c, x)\\
(c, yz)(d, xyz) &= (c\cdot d\gamma, x) &&= (d, xyz)(c, yz),
\end{aligned}$$

and let $(c, u)(d, v) = (cd, uv)$ for all other choices of u and v in W.

One readily verifies the following statements.

1. G is a commutative loop with normal subloop $A \times \langle 1\rangle$ isomorphic to A and with $G/A \cong W$.
2. If $G_1 = \langle A, x, y\rangle$, $G_2 = \langle A, x, z\rangle$ and $G_3 = \langle A, x, yz\rangle$, then the mapping $a \to ab \to b \to a$, $x \to x$ and $y \to z \to yz \to y$ induces an isomorphism of G_1 onto G_2, G_2 onto G_3 and G_3 onto G_1.
3. Every two elements of G generate a group of exponent 2; thus G is diassociative.
4. $\Phi(G_1) = \langle b\rangle$, $\Phi(G_2) = \langle a\rangle$ and $\Phi(G_3) = \langle ab\rangle$, so that $\Phi(G) = A$.
5. G is an N-loop. (Here one need only check that every proper subloop is of index 2 in another subloop.)
6. $Z(G_i) = \Phi(G_i)$ for $i = 1, 2, 3$, so that $Z(G) = 1$.

Thus G is a commutative, diassociative N-loop which is also a 2-loop but which is not nilpotent. One can show that a diassociative N-loop which is

not nilpotent must have order at least p^4 for some prime, p, and at least p^5 if p is 2. Thus our example is of minimal order. It seems plausible that an analogue of the construction given would produce examples for odd primes, but the work involved in checking condition (2) would be formidable.

4. Some results on Moufang loops

The outstanding result to date on Moufang loops is Bruck's theorem implying that commutative, Moufang loops are locally, finitely, centrally nilpotent [1, p. 157]. Thus, in particular, (4) implies (1) for finitely generated Moufang loops. In view of Theorem 2, in order to show that (2) implies (1) for finite Moufang loops, one may restrict attention to p-loops. We shall show that finite Moufang N-loops which are 2-loops or 3-loops are nilpotent.

Some of the difficulty in treating larger primes stems from the fact that, although (6) is amenable to proofs by induction, (6′) is not nearly so easy to work with. If we wish to base a proof on Lemma 3, then we must have some guarantee that G (and perhaps its maximal subloops, as well) satisfies (6′). We shall give a family of examples of Moufang p-loops which satisfy (6′) but not (6). In view of the examples, there would seem to be little hope of using (6) to solve the problem for Moufang loops.

PROPOSITION 6. *If G is a Moufang loop with normal subloop H, and if $T(H) = \{x \in Z(H) \mid x^2 = 1\}$, then $T(H)$ is a normal subloop of G.*

Proof. $T(H)$ is a subgroup of $Z(H)$, so that $T(H)$ is a subloop of G. If θ is an inner mapping of G, and if $m \in H$ and $x \in T(H)$ then, since θ is a semi-automorphism of G,

$$m = (m\theta^{-1})\theta = (x \cdot m\theta^{-1} \cdot x)\theta = x\theta \cdot m \cdot x\theta.$$

In particular, $1 = x\theta \cdot 1 \cdot x\theta$, so that $x\theta = (x\theta)^{-1}$ and $m \cdot x\theta = x\theta \cdot m$. But also if $m' \in H$, then

$$x\theta \cdot mm' = x\theta[m(x\theta \cdot m' \cdot x\theta)] = x\theta[([m \cdot x\theta]m')x\theta]$$
$$= (m \cdot x\theta)m' = (x\theta \cdot m)m'.$$

Thus $x\theta$ is in the nucleus of H. It follows that $x\theta \in T(H)$.

THEOREM 7. *A finite, Moufang 2-loop which is also an N-loop is centrally nilpotent.*

Proof. Let G be a minimal counterexample. Since G satisfies (i), (ii) and (iii) of Lemma 3 but not the conclusion of the lemma, it will suffice to show that G satisfies (6′) in order to reach a contradiction. Now if M is a non-trivial, maximal subloop of G, then in view of the minimality of G, M is nilpotent, so that $T(M)$ is a non-trivial, normal subloop of G contained in $Z(M)$. Hence, G satisfies (6′), as desired.

We have just used the fact that in a Moufang loop every inner mapping

is a semi-automorphism. In dealing now with the prime 3, we shall use the fact that every inner mapping is a pseudo-automorphism.

PROPOSITION 8. *Let G be a Moufang loop with normal subloop H. If θ is an inner mapping of G which (as a pseudo-automorphism of G) has a companion, c, in H, then $Z(H)\theta = Z(H)$.*

Proof. It is noted in [3, p. 62] that θ^{-1} has companion $d = (c\theta^{-1})^{-1}$, which also belongs to H. If $m \in H$ and $z \in Z(H)$, then

$$(m\theta \cdot z\theta)\theta^{-1} \cdot d = m \cdot zd = mz \cdot d,$$

so that $m\theta \cdot z\theta = (mz)\theta$. Similarly, $z\theta \cdot m\theta = (zm)\theta$, so that $(z\theta, m\theta) = 1$. If also $m' \in H$, then

$$\begin{aligned}[m\theta(z\theta \cdot m'\theta)]\theta^{-1} \cdot d &= m(zm' \cdot d) = mz \cdot m'd = [(mz)\theta \cdot m'\theta]\theta^{-1} \cdot d \\ &= [(m\theta \cdot z\theta)m'\theta]\theta^{-1} \cdot d,\end{aligned}$$

so that $(m\theta, z\theta, m'\theta) = 1$. Since $m\theta$ and $m'\theta$ are typical members of H, $z\theta \in Z(H)$.

THEOREM 9. *If G is a finite Moufang 3-loop which is also an N-loop, then G is centrally nilpotent.*

Proof. Let G be a minimal counterexample. As in the proof of Theorem 7, it will suffice to show that G satisfies (6′). But if M is maximal in G, then M contains (x, y) and x^3 for every x and y in G, so that M contains a companion for each inner mapping of G. In view of Proposition 8, $Z(M) \lhd G$. Since every maximal subloop of G is nilpotent, G satisfies (6).

The following construction gives a collection of examples of Moufang p-loops satisfying (6′) but not (6). In addition to the comments made above, one may also note that the device of considering $\{x \in Z(M) \mid x^p = 1\}$ fails to help for these examples, since the loops constructed are of exponent p.

Let p be a prime greater than 3. Let

$$G = \{(i, j, k, l, m) \mid 0 \leq i, j, k, l, m < p\},$$

and define multiplication in G by

$$\begin{aligned}&(i, j, k, l, m) \cdot (i', j', k', l', m') \\ &\qquad = (i + i', j + j', k + k', l + l' + a_1, m + m' + a_2),\end{aligned}$$

where $a_1 = i'k$ and $a_2 = 6j'l + i(jk' - j'k) + i'(4j'k + 2jk' + 3jk)$, and where addition is modulo p.

As tedious computation would show, G is a Moufang loop of exponent p. Letting $x = (1, 0, 0, 0, 0)$, $y = (0, 1, 0, 0, 0)$, $z = (0, 0, 1, 0, 0)$, $u = (0, 0, 0, 1, 0)$ and $v = (0, 0, 0, 0, 1)$, one easily checks that $u = (z, x)$, $v = (x, y, z)$ and $(u, y) = v^6$. Routine computation shows that $G/\langle v\rangle$ and $\langle y, z, u, v\rangle$ are groups, that $Z(G) = \langle v\rangle$ and that $Z(\langle y, z, u, v\rangle) = \langle z, v\rangle$. Since

$(z, x) = u \notin Z(\langle y, z, u, v\rangle)$, it follows that G does not satisfy (6). Finally, G is nilpotent of class 3, since $Z(G) = \langle v\rangle$ and $Z(G/\langle v\rangle) = \langle u, v\rangle/\langle v\rangle$.

It can be shown that a Moufang p-loop of order p^4 or less is necessarily a group, so that the examples constructed are of minimal order. Moreover, this observation removes the necessity of proving that $G/\langle v\rangle$ and $\langle y, z, u, v\rangle$ are groups.

Certainly, the results of this section are far from adequate, but perhaps they indicate the difficulty of solving the problem for Moufang loops. My current conjecture is that every finite, Moufang p-loop which is also an N-loop is nilpotent. If anyone knows of an example to the contrary, I would greatly appreciate learning of it.

Added in Proof (March 3, 1965). Glauberman has shown (in work to appear elsewhere) that every finite, Moufang p-loop is nilpotent in case p is an odd prime. It can be shown that every finite, solvable, Moufang 2-loop is nilpotent. Whether or not "solvable" is redundant appears to be an open question.

Bibliography

1. R. H. Bruck, *A survey of binary systems*, Berlin-Göttingen-Heidelberg, Springer Verlag, 1958.
2. ———, *Contributions to the theory of loops*, Trans. Amer. Math. Soc., vol. 60 (1946), pp. 245–354.
3. ———, *Some theorems on Moufang loops*, Math. Zeitschrift, vol. 73 (1960), pp. 59–78.
4. R. H. Bruck, and Lowell J. Paige, *Loops whose inner mappings are automorphisms*, Ann. of Math. (2), vol. 63 (1956), pp. 308–323.
5. A. G. Kurosh, *The theory of groups, vol. 2*, translated by K. A. Hirsch, Chelsea, New York, 1956.
6. D. A. Norton, *Hamiltonian loops*, Proc. Amer. Math. Soc., vol. 3 (1952), pp. 56–65.

University of Oregon
Eugene, Oregon