Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Algebra 273 (2004) 288–294

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

Finite loops with dihedral inner mapping groups are solvable

Markku Niemenmaa

Department of Mathematical Sciences, University of Oulu, PL 3000, 90014 Oulu, Finland

Received 23 September 2002

Communicated by Robert Kottwitz

1. Introduction

Let Q be a groupoid with a neutral element e. We say that Q is a loop provided that each of the two equations $ax = b$ and $ya = b$ has a unique solution for any $a, b \in Q$. If a loop Q is associative, then Q is in fact a group (this is the reason why loops are sometimes called nonassociative groups). In a loop Q the mappings $L_a(x) = ax$ (left translation) and $R_a(x) = xa$ (right translation) are permutations on Q for every $a \in Q$. The permutation group $M(Q) = \langle L_a, R_a\colon a \in Q\rangle$ is called the multiplication group of the loop Q. Clearly, $M(Q)$ is transitive on Q. The stabilizer of the neutral element e is denoted by $I(Q)$ and this stabilizer is called the inner mapping group of the loop Q. The definitions of the multiplication group and the inner mapping group were given by Bruck [1] in an article that was published in 1946. In this article, which was fundamental for loop theory, Bruck also defined solvability in loops in the following way: a loop Q is solvable if it has a series $1 = Q_0 \subseteq \cdots \subseteq Q_n = Q$, where Q_{i-1} is a normal subloop of Q_i and Q_i/Q_{i-1} is an abelian group. Normal subloops are naturally kernels of loop homomorphisms.

By using the notions of the multiplication group and the inner mapping group of a loop, we get a very strong link between loop theory and group theory and one of the main targets here is to consider the relation between the structure of the loop and the structure of the corresponding group. Bruck was able to show that the group theoretical nilpotency of the multiplication group $M(Q)$ implies the loop theoretical solvability of the loop Q. After this, it was only in 1996 that Vesanen [22] managed to prove the following important and deep result: if Q is a finite loop such that the multiplication group $M(Q)$ is a solvable group, then Q is a solvable loop. This result opens a large variety of possibilities to our investigations. One direction is to study those properties of the inner mapping group $I(Q)$

E-mail address: mniemen@cc.oulu.fi.

doi:10.1016/j.jalgebra.2002.09.001

which guarantee the solvability of the multiplication group $M(Q)$ (and thus, in the finite case, the solvability of the loop Q).

A series of papers [3,4,10,13–17] by Csörgö, Kepka, Myllylä and Niemenmaa (between 1990 and 2000) showed us that the solvability of $M(Q)$ follows provided that $I(Q)$ is cyclic, finite abelian, dihedral of order 2^n or dihedral of order $2k$, where k is an odd number. The purpose of this paper is to show that the following more general result holds: if $I(Q)$ is a finite dihedral group, then $M(Q)$ is a solvable group and, in the finite case, Q is a solvable loop.

In [16] Kepka and Niemenmaa showed that many properties of loops and their multiplication groups can be reduced to the properties of connected transversals in groups. Therefore in Section 2 we discuss these transversals and introduce the reader the theorem that gives a purely group theoretical characterization of multiplication groups of loops by using connected transversals.

In Section 3 we prove our main results. First we prove the following group theoretical result: if G is a group with a finite dihedral subgroup H and with H-connected transversals, then G is solvable. In the proof we need some understanding about the structure of nonsolvable finite groups with Sylow 2-subgroups which are dihedral, semidihedral, quaternion or generalized quaternion. The needed results can be found in the articles by Glauberman [5], Gorenstein and Walter [7] and Wong [23]. After this we give a loop theoretical interpretation of our group theoretical results.

Our notation in group theory is standard and follows [6] and [8]. For basic facts about loop theory and its history the reader is advised to consult the articles by Bruck [1], Pflugfelder [18] and Smith [20]. For more recent results in loop theory we recommend the articles by Kinyon, Kunen and Phillips [11,12,19].

2. Connected transversals

Let Q be a loop and denote $A = \{L_a\colon a \in Q\}$ and $B = \{R_a\colon a \in Q\}$. The two sets A and B are left (and also right) transversals to $I(Q)$ in $M(Q)$. Simple calculations show that the commutator subgroup $[A, B]$ is contained in $I(Q)$ and we say that A and B are $I(Q)$-connected transversals in $M(Q)$. Generally speaking, if G is a group with a subgroup H and with two left transversals A and B to H in G such that $[A, B] \leqslant H$, then we say that A and B are H-connected transversals in G. In the following two lemmas we assume that A and B are H-connected transversals in G. By H_G we denote the largest normal subgroup of G contained in H and we say that H_G is the core of H in G.

Lemma 2.1. *The sets A^g and B^g are left (right) transversals to H in G for every $g \in G$.*

Lemma 2.2. *If $C \subseteq A \cup B$ and $K = \langle H, C\rangle$, then $C \subseteq K_G$.*

For the proofs, see [16, Lemmas 2.1 and 2.5].

In 1990, Kepka and Niemenmaa [16, Theorem 4.1] proved the following theorem that gives a purely group theoretical characterization of multiplication groups of loops.

Theorem 2.3. *A group G is isomorphic to the multiplication group of a loop if and only if there exist a subgroup H satisfying $H_G = 1$ (thus the core of H in G is trivial) and H-connected transversals A and B such that $G = \langle A, B\rangle$.*

We conclude this section by the following result of Vesanen [21, Chapters 3 and 4].

Theorem 2.4. *If $G = PSL(2, q)$, where $q \geqslant 5$ is odd, then G does not have connected transversals to dihedral subgroups.*

3. Main results

We are now ready to prove our main result.

Theorem 3.1. *Assume that G is a finite group, H a dihedral subgroup of G and assume further that there exist H-connected transversals in G. Then G is a solvable group.*

Proof. From [15] and [13] it follows that the claim is true if H is a 2-group or if $|H| = 2k$, where k is an odd number. Thus here we may assume that $|H| = 2^t k$, where $t \geqslant 2$ and $k \geqslant 3$ is an odd number.

Let G be a minimal counterexample. If $H_G > 1$, then H/H_G is either cyclic or dihedral, hence G/H_G and G are solvable. Thus we may assume that $H_G = 1$. If H is not a maximal subgroup of G, then there is a proper subgroup T of G such that $H < T$. By Lemma 2.2, $T_G > 1$. Since HT_G/T_G is either cyclic or dihedral, we may conclude that G/T_G is solvable. By induction, T is solvable, which means that G is solvable. Thus we may assume that H is a maximal subgroup of G. It is also clear that $N_G(H) = H$.

We now divide the proof into two parts: in the first part we assume that the order of H is $2^t k$, where $t \geqslant 3$ and in the second part we assume that the order of H is $4k$.

(1) Let $|H| = 2^t k$, where $t \geqslant 3$ and $k \geqslant 3$ is odd. Assume then that Q is a Sylow 2-subgroup of H. If Q is not a Sylow 2-subgroup of G, then we have a 2-subgroup D of G such that $Q < D$ and $[D : Q] = 2$. The subgroup Q is dihedral and since $t \geqslant 3$ it has a cyclic characteristic subgroup R of order 2^{t-1}. Since R is normal in H and in D and H is maximal in G, it follows that R is normal in G. This is not possible, as $H_G = 1$.

Thus we may assume that Q is a dihedral Sylow 2-subgroup of G. If G is simple, then we apply [7] and it follows that either $G \cong PSL(2, q)$ ($q \geqslant 5$ odd) or $G \cong A_7$. From Theorem 2.4 we see that the groups $PSL(2, q)$ do not have connected transversals to dihedral subgroups. It is also easy to check that the alternating group A_7 does not have a dihedral maximal subgroup. This means that G is not simple and there exists a nontrivial minimal normal subgroup N in G. Clearly, N is not contained in H, hence $G = NH$.

Denote by L the cyclic subgroup of H of order $2^{t-1}k$. Since $N \cap H$ is normal in H, it follows that either $N \cap H \leqslant L$ or $N \cap H$ is a dihedral group of order $2^{t-1}k$. If $N \cap H \leqslant L$, then we write $E = NL$. Now E is a proper subgroup of G, $N_E(L) = L$ and since $H_G = 1$, we may conclude that $L \cap L^e = 1$ for every $e \in E - L$. Thus E is a Frobenius group with a Frobenius complement L, hence the groups E, N and G are solvable (for the properties of Frobenius groups, see [8, pp. 495–507]). There remains the case that $N \cap H$ is a dihedral group of order $2^{t-1}k$ and $[G : N] = 2$. Of course, N has a dihedral Sylow 2-subgroup of order 2^{t-1}.

Now we wish to show that N is simple. Assume that N is not simple and let $K < N$ be a maximal normal subgroup of N. Let $L = \langle x\rangle$ be the cyclic subgroup of H of order $2^{t-1}k$. Then $G = N\langle x\rangle$, $x^2 \in N$ and the subgroup K has two conjugates K and K^x in G. As $K_G = K \cap K^x$ is normal in G, it follows that $K \cap K^x = 1$. Then $N = KK^x$ and $|N| = |K|^2$. If p is an odd prime which divides k, then p divides $|N|$ and $|K|$. Thus K has a Sylow p-subgroup S. If P is the Sylow p-subgroup of H, then P is also a Sylow p-subgroup of N and there exists $n \in N$ such that $S^n \leqslant P \leqslant \langle x\rangle$. Clearly, $S^n \leqslant K^n = K$ and $(S^n)^x = S^n \leqslant K^x$. But then $S^n \leqslant K \cap K^x = 1$, a contradiction. We conclude that N is a simple group.

Since N has a dihedral Sylow 2-subgroup, we can again apply [7] and it follows that either $N \cong PSL(2, q)$ ($q \geqslant 5$ is odd) or $N \cong A_7$.

If $N \cong A_7$, then $N \cap H$ would be dihedral of order $8k$ and A_7 would contain an element of order $4k$. This is not possible and we may concentrate on the case where $N \cong PSL(2, q)$. For the structure of the groups $PSL(2, q)$ and their subgroups we advise the reader to consult [8, pp. 191–213]). For this proof we need to know that $PSL(2, q)$ has dihedral subgroups of order $q \pm 1$ and these subgroups are in the role of $N \cap H$. Furthermore, the orders of the elements of $PSL(2, q)$ divide q or $(q \pm 1)/2$.

Now $|N| = (q+1)q(q-1)/2$, $|G| = 2|N|$, $|H| = 2(q\pm 1)$ and $|A| = |B| = q(q\mp 1)/2$. If $A \cup B \subseteq N$, then A and B are $(N \cap H)$-connected transversals in N and by induction, we conclude that N is solvable. This is not possible, hence we may assume that there exists $a \in A \cup B - N$. Of course, $a^2 \in N$.

If $|a| = 2^d r$, where $d \geqslant 2$ and r is odd, then $|a^r| = 2^d$ and $a^r \in Q^g \leqslant H^g$ for some $g \in G$ (remember that $Q \leqslant H$ is a Sylow 2-subgroup of G). Further, $a^r \in H^g \cap H^{ga}$, hence $\langle a^r\rangle$ is normal in $\langle H^g, H^{ga}\rangle = G$. This is not possible, so we may assume that $|a| = 2r$, where $r > 1$ is odd. (If $|a| = 2$, then $a^g \in H$ for some $g \in G$ contradicting Lemma 2.1.)

Now assume that $|H| = 2(q + 1)$, $|N \cap H| = q + 1$ and $|A| = |B| = q(q - 1)/2$. Since $4k$ divides $q + 1$, we may assume that either $q = 11$ or $q \geqslant 19$.

Since $a^2 \in N$, it follows that $|a^2|$ divides q or $(q \pm 1)/2$. In any case, $|C_G(a)| \leqslant 2q$. Since $G' \leqslant N$, it follows that $a^{-1}b^{-1}ab \in N \cap H$ for every $b \in B$ and thus $a^b \in a(N \cap H)$ for every $b \in B$. Let b and t be two different elements from B. If $a^b = a^t$, then $1 \neq bt^{-1} \in C_G(a)$.

Thus we place $|A| - |N \cap H| = q(q - 1)/2 - (q + 1)$ elements in the set $E = C_G(a) - \{1\}$, which has at most $2q - 1$ elements. Clearly, there exists $c \in E$ such that $c = b_1b_2^{-1} = b_3b_4^{-1}$. Thus $b_1 = cb_2$ and $b_3 = cb_4$. If $d \in A$, then $[d, cb_i] = [d, b_i][d, c]^{b_i} \in H$, hence $[d, c] \in H^{b_i^{-1}}$ $(i = 2, 4)$.

But then $[d, c]$ is in the intersection of two different conjugates of H. Since this intersection has at most four elements, we are placing $q(q - 1)/2$ commutators of type $[d, c]$ in the four places of the intersection and therefore we have an element h such that $h = [d_1, c] = \cdots = [d_f, c]$, where $f \geqslant q(q - 1)/8$ and the elements d_i are from A. If $[d_1, c] = [d_2, c]$, then $d_1d_2^{-1} \in C_G(c)$ and we are placing $f - 1$ elements in the set $C_G(c) - \{1\}$, which has at most $2q - 1$ elements.

Now $f - 1 \geqslant q(q-1)/8 - 1$ and if $q \geqslant 19$, then $f - 1 > 2q - 1$. But then $d_1 d_i^{-1} = d_1 d_j^{-1}$ for some $i \neq j$ and we have a contradiction.

We still have to consider the case where $q = 11$ and $N \cong PSL(2, 11)$. Then $|H| = 24$, $|N \cap H| = 12$ and $|A| = |B| = 55$. Since $|a| = 2r$, where $r > 1$ is odd and $|a^2|$ divides 11, 6 or 5, we conclude that $|a| = 6$, 10 or 22. If $|a| = 6$ or $|a| = 10$, then $|C_G(a)| \leqslant 10$ and calculations similar to the ones in the preceding section lead us to a contradiction.

Then assume that $|a| = 22$. Now a^{11} is an involution belonging to $H^g - N$ for some $g \in G$ and $C_N(a^{11}) \geqslant \langle a^2, z\rangle$, where $z \in Z(H^g)$. Then 22 divides the order of $C_N(a^{11})$ and by looking at the maximal subgroups of $PSL(2, 11)$ we may conclude that $C_N(a^{11}) = N$. As $G = N\langle a^{11}\rangle$, we conclude that $a^{11} \in Z(G)$. But this is not possible as H^g has a trivial core.

In the case that $|H| = 2(q-1)$, $|N \cap H| = q - 1$ and $|A| = |B| = q(q+1)/2$, we may proceed in a similar way. Now we are ready with the first part and it is time to begin the second part of our proof.

(2) Let $|H| = 4k$, where $k > 1$ is an odd number. If 8 does not divide $|G|$, then the Sylow 2-subgroups of G are of order four. If G is simple, then we use [7] and it follows that $G \cong PSL(2, q)$, where $q \geqslant 5$ is odd. By Theorem 2.4 we know that G does not have connected transversals to dihedral subgroups. Then assume that G is not simple and let N be a minimal normal subgroup of G. As in the first part of the proof we may conclude that N is simple and $[G : N] = 2$. But now N has a Sylow 2-subgroup of order 2 contradicting the simplicity of N.

Thus we may assume that 8 divides $|G|$. Let S be a Sylow 2-subgroup of G such that $|S \cap H| = 4$. Now $Z(H) = \{1, t\}$, where t is an involution. Since $H_G = 1$ and H is maximal in G it follows that $C_S(t) = S \cap H$. From [9, p. 316] it follows that S is either dihedral or semidihedral.

If S is semidihedral and G is simple, then [23, Theorem 2] applies and the involutions in G form a single conjugacy class. As $Z(S) \leqslant H$, it follows that if $u \in Z(S)$ is an involution, then $t = u^g \in Z(S^g)$ for some $g \in G$. But then $C_G(t) \geqslant (H, S^g) = G$ and $H_G > 1$, a contradiction. If S is semidihedral and G is not simple, then we conclude from [23] that we have a normal subgroup N of G such that $[G : N] = 2$. Calculations similar to those in the first part of our proof show that N is simple. Now $[S : S \cap N] = 2$ and as a maximal subgroup of S, the subgroup $S \cap N$ is either cyclic, quaternion, generalized quaternion or dihedral (see [6, p. 191]). A Sylow 2-subgroup of a simple group cannot be cyclic and by combining [8, pp. 624–627] and [5] the same is true for generalized quaternion groups. All this means that $S \cap N$ has to be dihedral.

If we assume that S is dihedral, then we can use [7] and Theorem 2.4 to deduce that G is not simple and as before, G has a normal subgroup N of index 2, N is simple and $S \cap N$ is dihedral.

Thus from [7] it follows that either $N \cong PSL(2, q)$, where $q \geqslant 5$ is odd or $N \cong A_7$. First assume that $N \cong PSL(2, q)$. We know that $|H \cap N| = 2k$ and $H \cap N$ is a dihedral subgroup. If $A \cup B \subseteq N$, then A and B are $N \cap H$-connected transversals in N. By [13], N is solvable. As this is not possible we may assume that there exists $a \in A \cup B - N$. Then $a^2 \in N$ and $C_G(a)$ has at most $2q$ elements.

Assume that $|N \cap H| = q + 1$ (then $|A| = |B| = q(q-1)/2$). Now $2k = q + 1$ and it follows that either $q = 5$ or $q \geqslant 9$. We now employ the commutator-centralizer method and the notation that was used in the first part of our proof. If $d \in A$, then we have an element $c \in C_G(a) - \{1\}$ such that the commutator $[d, c]$ is in the intersection of two different conjugates of $N \cap H$. Obviously, this intersection has at most two elements. If $[d, c] = 1$, then $d \in C_G(c) - \{1\}$. Thus at least $q(q-1)/2 - (2q-1) = (q^2 - 5q + 2)/2$ elements of the form $[d, c]$ are equal to the involution in the intersection. It follows that we are placing $(q^2 - 5q + 2)/2 - 1$ elements in the set $C_G(c) - \{1\}$. The set has at most $2q - 1$ elements, hence we get a contradiction when $q \geqslant 9$.

The case where $q = 5$ has to be investigated separately. So assume that $N \cong PSL(2, 5)$, $|H| = 12$, $|H \cap N| = 6$ and $|A| = |B| = 10$. As before, we assume that there exists $a \in A \cup B - N$. Then $a^2 \in N$ and $|a| = 4$, 6 or 10. If $|a| = 10$, then $G = \langle a \rangle H$ and by [2], G is solvable. Clearly, $|a| = 6$ is not possible as $|N \cap H| = 6$. Thus we must have $a \in A$ such that $|a| = 4$ and $|C_G(a)| = 4$. Now the centralizer-commutator calculations lead us to a contradiction.

If $|H \cap N| = q - 1$ and $|A| = |B| = q(q+1)/2$ then we can proceed in a similar way. Thus finally assume that $N \cong A_7$. Now $|H \cap N| = 2k$ and by looking at the subgroups of A_7 we conclude that $|H \cap N| \leqslant 10$. Then $|H| \leqslant 20$ and $|A| = |B| \geqslant 252$. Again, calculations based on the numbers of commutators and the size of centralizers give us a contradiction. This is our final contradiction and so the proof is complete. □

After this we shall have a look at the loop theoretical consequences of Theorem 3.1. We are interested in solvable loops (as defined in the introduction) and we have the following important solvability criterion proved by Vesanen [22].

Theorem 3.2. *If Q is a finite loop whose multiplication group is solvable, then Q is a solvable loop.*

The relation between multiplication groups of loops and connected transversals was given in Theorem 2.3. By combining this result with Theorems 3.1 and 3.2, we immediately have

Theorem 3.3. *If Q is a finite loop whose inner mapping group is a dihedral group, then Q is a solvable loop.*

References

[1] R.H. Bruck, Contributions to the theory of loops, Trans. Amer. Math. Soc. 60 (1946) 245–354.
[2] J. Carr, A solubility criterion for factorised groups, Arch. Math. 27 (1976) 225–231.
[3] P. Csörgö, M. Niemenmaa, Solvability conditions for loops and groups, J. Algebra 232 (2000) 336–342.
[4] P. Csörgö, K. Myllylä, M. Niemenmaa, On connected transversals to dihedral subgroups of order $2p^n$, Algebra Colloq. 7 (1) (2000) 105–112.
[5] G. Glauberman, On groups with a quaternion Sylow 2-subgroup, Illinois J. Math. 18 (1974) 60–65.
[6] D. Gorenstein, Finite Groups, Harper & Row, New York, 1968.
[7] D. Gorenstein, J.H. Walter, The characterization of finite groups with dihedral Sylow 2-subgroups, J. Algebra 2 (1965) 85–151; J. Algebra 2 (1965) 218–270; J. Algebra 2 (1965) 354–393.
[8] B. Huppert, Endliche Gruppen I, Springer-Verlag, Berlin, 1967.
[9] B. Huppert, N. Blackburn, Finite Groups III, Springer-Verlag, Berlin, 1982.

[10] T. Kepka, M. Niemenmaa, On loops with cyclic inner mapping groups, Arch. Math. 60 (1993) 233–236.
[11] M. Kinyon, K. Kunen, J.D. Phillips, Every diassociative A-loop is Moufang, Proc. Amer. Math. Soc. 130 (3) (2002) 619–624.
[12] K. Kunen, Quasigroups, loops and associative laws, J. Algebra 185 (1996) 194–204.
[13] K. Myllylä, On connected transversals to dihedral subgroups, Acta Univ. Oulu. A 350 (2000) 1–23.
[14] M. Niemenmaa, Transversals, commutators and solvability in finite groups, Boll. Un. Mat. Ital. A (7) 9 (1995) 203–208.
[15] M. Niemenmaa, On loops which have dihedral 2-groups as inner mapping groups, Bull. Austral. Math. Soc. 52 (1995) 153–160.
[16] M. Niemenmaa, T. Kepka, On multiplication groups of loops, J. Algebra 135 (1990) 112–122.
[17] M. Niemenmaa, T. Kepka, On connected transversals to abelian subgroups, Bull. Austral. Math. Soc. 49 (1994) 121–128.
[18] H.O. Pflugfelder, Historical notes on loop theory, Comment. Math. Univ. Carolin. 41 (2) (2000) 359–370.
[19] J.D. Phillips, A note on simple groups and simple loops, in: Proceedings of the Groups, Korea, 1998, de Gruyter, Berlin, 2000, pp. 305–317.
[20] J.D.H. Smith, Loops and quasigroups: aspects of current work and prospects for the future, Comment. Math. Univ. Carolin. 41 (2000) 415–427.
[21] A. Vesanen, On connected transversals in $PSL(2, q)$, Ann. Acad. Sci. Fenn. Math. Diss. 84 (1992).
[22] A. Vesanen, Solvable loops and groups, J. Algebra 180 (1996) 862–876.
[23] W.J. Wong, On finite groups whose 2-Sylow subgroups have cyclic subgroups of index 2, J. Austral. Math. Soc. 4 (1) (1964) 90–112.