ON FINITE LOOPS
WHOSE INNER MAPPING GROUPS ARE ABELIAN

MARKKU NIEMENMAA

Loops are nonassociative algebras which can be investigated by using their multi-plication groups and inner mapping groups. If the inner mapping group of a loop is finite and Abelian, then the multiplication group is a solvable group. It is clear that not all finite Abelian groups can occur as inner mapping groups of loops. In this paper we show that certain finite Abelian groups with a special structure are not isomorphic to inner mapping groups of finite loops. We use our results and show how to construct solvable groups which are not isomorphic to multiplication groups of loops.

1. INTRODUCTION

If Q is a groupoid, then we say that Q is a loop if Q has a neutral element e and each of the two equations $ax = b$ and $ya = b$ has a unique solution for any $a, b \in Q$. The mappings $L_a(x) = ax$ (left translation) and $R_a(x) = xa$ (right translation) are permutations on Q for every $a \in Q$ and the permutation group $M(Q) = \langle L_a, R_a : a \in Q \rangle$ is called the *multiplication group* of Q. It is obvious that $M(Q)$ is transitive in Q and the stabilisers of elements of Q are conjugated in $M(Q)$. The stabiliser of the neutral element e is denoted by $I(Q)$ and this subgroup of $M(Q)$ is called the *inner mapping group* of Q. These two notions linking loops to groups were defined by Bruck [2] and he was the first to investigate the structure of loops by using group theory.

In this paper, which is a continuation of [6, 7, 9, 10], we are interested in the structure of inner mapping groups of loops. In [11] we managed to prove that if $I(Q)$ is a finite Abelian group, then $M(Q)$ is solvable. Now it is clear that some finite Abelian groups can occur as inner mapping groups of loops while other finite Abelian groups are never isomorphic to inner mapping groups of loops. We thus started to investigate the following problem: Which finite Abelian groups are (are not) isomorphic to inner mapping groups of loops? It is not very difficult to see that $I(Q) = 1$ if and only if Q is an Abelian group. We also know [7, 10] that $I(Q)$ is cyclic if and only if Q is an Abelian group. In [9] we showed that for a finite loop Q, $I(Q)$ can not be isomorphic to $C_n \times D$, where C_n is a cyclic group of order n and D is a finite Abelian group

such that n and $|D|$ are relatively prime. Later on, Kepka [6] managed to show that this result is true for infinite loops, too. The purpose of this paper is to show that the following two results hold:

(1) If Q is a finite loop, then $I(Q)$ is never isomorphic to the direct product $C_{p^k} \times C_p$, where p is an odd prime number and $k \geqslant 2$.

(2) Let Q be a finite loop and $p \neq q$ be two prime numbers such that p is odd and q does not divide $|Q|$. Then $I(Q)$ is not isomorphic to $\left(C_{p^k} \times C_p \right) \times D$, where $k \geqslant 2$ and D is an Abelian q-group.

Here we wish to point out that if Q is a group, then $I(Q)$ is the group of inner automorphisms of Q. The question which finite Abelian groups occur as inner automorphism groups of groups was completely solved by Baer [1].

Many properties of loops can be reduced to the properties of connected transversals in the multiplication group. The notion of connected transversals was introduced by Kepka and Niemenmaa [10] in 1990 and since then it has been at the heart of much of the current research on loops and their relation to groups. This paper is no exception: we apply the theory of connected transversals when proving our main results. Section 2 contains basic information about connected transversals, gives the characterisation theorem of multiplication groups of loops and contains other preliminary results which are needed later. In Section 3 we prove our main results, first in purely group theoretical terms (using connected transversals), and after that we give the loop theoretical interpretation of our results in Section 4. Finally, by using this information, we show how to construct examples of solvable groups which are not isomorphic to multiplication groups of loops.

Our notation is standard. For a general overview about the relation between loops and groups we refer to [2, 10, 13, 14, 15]. The reader interested in the history of loop theory should have a look at the article by Pflugfelder [12] and those who wish to know about the applications of nonassociative algebras are advised to read the articles [3, 4, 8].

2. GROUPS, LOOPS AND CONNECTED TRANSVERSALS

Let Q be a loop and consider the groups $M(Q)$ and $I(Q)$ and the left and right translations defined in the introduction. If we write $A = \{L_a : a \in Q\}$ and $B = \{R_a : a \in Q\}$, then the commutator subgroup $[A, B] \leqslant I(Q)$ and A and B are left transversals to $I(Q)$ in $M(Q)$. If $1 < K \leqslant I(Q)$, then K is not a normal subgroup of $M(Q)$. Finally, $M(Q) = \langle A, B \rangle$.

We then consider the corresponding situation in groups in general. Let H be a subgroup of G and let A and B be two left transversals to H in G. We say that A and B are H-connected if $[A, B] \leqslant H$. In fact, H-connected transversals are both left

and right transversals ([**10**, Lemmas 2.1 and 2.2]). By H_G we denote the core of H in G, that is, the largest normal subgroup of G contained in H. If $H_G = 1$, we say that H is core-free in G. The relation between multiplication groups of loops and connected transversals is given by

THEOREM 2.1. *A group G is isomorphic to the multiplication group of a loop if and only if there exist a subgroup H satisfying $H_G = 1$ and H-connected transversals A and B such that $G = \langle A, B \rangle$.*

For the proof, see [**10**, Theorem 4.1].

In the following lemmas we assume that A and B are H-connected transversals in G.

LEMMA 2.2. *If $H_G = 1$, then $N_G(H) = H \times Z(G)$.*

LEMMA 2.3. *If $C \subseteq A \cup B$ and $K = \langle H, C \rangle$, then $C \subseteq K_G$.*

LEMMA 2.4. *If $H_G = 1$, then $Z(G) \subseteq A \cap B$.*

For the proofs, see [**10**, Lemma 2.5 and Proposition 2.7] and [**7**, Lemma 1.4]. The reader should observe that from Lemma 2.3 it immediately follows that $K = K_G H$. In the following four lemmas we assume that $G = \langle A, B \rangle$. As usual, p denotes a prime number.

LEMMA 2.5. *If H is a cyclic subgroup of G, then $G' \leqslant H$.*

LEMMA 2.6. *If $H \cong C_p \times C_p$, then $G' \leqslant N_G(H)$.*

LEMMA 2.7. *If G is a finite group and $H \cong C_n \times D$, where $n > 1$, D is Abelian and $\gcd(n, |D|) = 1$, then $H_G > 1$.*

LEMMA 2.8. *If G is a finite group and H is Abelian, then H is subnormal in G.*

For the proofs, see [**7**, Theorem 2.2], [**11**, Lemma 4.2], [**9**, Theorem 2.3], and [**9**, Lemma 2.1].

If G is a finite group, then the Frattini subgroup $\Phi(G)$ is the intersection of all maximal subgroups of G. Clearly, $\Phi(G)$ is a characteristic subgroup of G. We need

LEMMA 2.9. *If G is a p-group, then $\Phi(G) = G' \langle x^p : x \in G \rangle$.*

For the proof, see [**5**, pp. 272–273].

LEMMA 2.10. *If $[a, b]$ commutes with a and b, then $(ab)^n = a^n b^n [b, a]^{\binom{n}{2}}$.*

For the proof, see [**5**, pp. 253 - 254].

3. MAIN THEOREMS

Throughout this section we assume that G is a finite group, H is an Abelian

subgroup of G with a special structure and there exist H-connected transversals A and B such that $G = \langle A, B \rangle$.

THEOREM 3.1. *Let $H \cong C_{p^k} \times C_p$ where p is an odd prime number and $k \geqslant 2$. Then H_G is not trivial.*

PROOF: Let G be a counterexample of smallest possible order. Thus $H_G = 1$ and from Lemmas 2.2 and 2.8 it follows that $N_G(H) = H \times Z(G)$ and $Z(G) > 1$. If $z \in Z(G)$ and $|z| = r$ (r is a prime number), then by considering $G/\langle z \rangle$ and $H\langle z \rangle/\langle z \rangle$, we may assume that there exists a normal subgroup K of G such that $\langle z \rangle < K \leqslant H\langle z \rangle$ (here K is the largest normal subgroup of G contained in $H\langle z \rangle$). If $r \neq p$, then K has a Sylow p-subgroup which is normal in G, hence $H_G > 1$. Thus we may assume $r = p$ and we may conclude that $Z(G)$ is a p-group.

If K contains an element $x \in H$ of order p^l ($l \geqslant 2$), then by Lemma 2.9, $\Phi(K)$ is a nontrivial subgroup of H and $\Phi(K)$ is normal in G, which is not possible. Thus K is an elementary Abelian p-group. If $k \geqslant 3$, then we consider G/K and HK/K. If HK/K is cyclic, then it follows from Lemma 2.5 that $HK = H\langle z \rangle$ is normal in G, hence $\Phi(H\langle z \rangle)$ is normal in G. Since this is not possible, we use induction and conclude that there exists a normal subgroup L of G such that $K < L \leqslant HK = H\langle z \rangle$. As this is not possible, we may assume that $k = 2$.

We write $H = \langle y \rangle \times \langle x \rangle$, where $|y| = p^2$ and $|x| = p$. Thus $K = \langle y^p \rangle \times \langle z \rangle$ and HK/K is elementary Abelian of order p^2. From Lemma 2.6 we conclude that $G' \leqslant N_G(HK)$. In what follows, we denote the group $N_G(HK)$ by E. Clearly, E is normal in G. As the core of HK/K in G/K is trivial, it follows from Lemma 2.2 that $N_{G/K}(HK/K) = HK/K \times Z(G/K)$. We write $M/K = Z(G/K)$ and then $E = HKM$, where $HK \cap M = K$ and M is a normal subgroup of G. By Lemma 2.4, $Z(G/K) \subseteq AK/K \cap BK/K$ and thus $M \subseteq AK \cap BK$.

Now $E = CH = DH$, where $C \subseteq A$ and $D \subseteq B$. Furthermore, it is easy to see that $M \subseteq CK = DK$ and, by Lemma 2.4, we must have $M = C\langle y^p \rangle = D\langle y^p \rangle$. As HK is normal in E, it follows that $\Phi(HK) = \langle y^p \rangle$ is normal in E (and in M). Since $[C, D] \leqslant H \cap M = \langle y^p \rangle$, we have $M' \leqslant \langle y^p \rangle$. Since M' is normal in G, we conclude that $M' = 1$, hence M is an Abelian group. Thus $K = \langle y^p, z \rangle \leqslant Z(E)$.

Since $E' \leqslant HK$ and E' is normal in G, we conclude that $E' \leqslant K$. We write $W = \langle g \in E : g^p = 1 \rangle$. It is immediate that W contains x, y^p and z and W is a normal subgroup of G. If $g, h \in W$, then $(gh)^p = g^p h^p [h, g]^{\binom{p}{2}} = 1$ by Lemma 2.10 (remember that p is odd) and thus $W = \{g \in E : g^p = 1\}$. If we consider the group G/W and its cyclic subgroup HW/W, then it follows from Lemma 2.5 that $G' \leqslant HW$, which means that HW is normal in G. If $h \in H$ and $w \in W$, then we use Lemma 2.10 and get $(hw)^p = h^p w^p [w, h]^{\binom{p}{2}} = h^p \in \langle y^p \rangle$. Thus $(HW)^p = \langle t^p : t \in HW \rangle = \langle y^p \rangle$ and since $(HW)^p$ is a characteristic subgroup of HW, we conclude that $\langle y^p \rangle$ is normal

in G, a contradiction. The proof is complete.   ☐

The following two lemmas will be needed in the proof of Theorem 3.4.

LEMMA 3.2. *Let $p \neq q$ be two prime numbers. If $H \cong C_p \times D$, where D is an Abelian Sylow q-subgroup of G, then $G' \leqslant H$.*

PROOF: Let G be a minimal counterexample. By Lemma 2.7, $H_G > 1$. If $|H_G|$ divides $|D|$, then we are done by induction (or by Lemma 2.5). If $|H_G| = pt$, where $1 < t \leqslant |D|$, then we have a nontrivial subgroup K of D which is normal in G and again we are ready. We still have to consider the case $|H_G| = p$. Let $F = N_G(D)$ and let M be a maximal subgroup of G such that $M \geqslant F$. Clearly, $F \geqslant H$. If $H = M$, then from Lemma 2.8 it follows that H is normal in G, hence $G' \leqslant H$. If $H < M$, then we use Lemma 2.3 and get $M_G > 1$. Thus $HM_G/M_G = M/M_G$ is subnormal in G/M_G by Lemma 2.8, which means that M is normal in G. By the Frattini argument, $G = MN_G(D) = M$, a contradiction. Thus $G = F$ and it follows that D is normal in G. But then $H = H_GD$ is normal in G and $G' \leqslant H$.   ☐

LEMMA 3.3. *Let $p \neq q$ be two prime numbers. If $H \cong (C_p \times C_p) \times D$, where D is an Abelian Sylow q-subgroup of G, then $G' \leqslant N_G(H)$.*

PROOF: Our proof is by induction on $|G|$ and we first assume that $H_G > 1$. By using Lemmas 2.5, 2.6 and 3.2 and the fact that G is a minimal counterexample, we may conclude that $G' \leqslant N_G(H)$ with one exception: the case $H_G \cong C_p \times C_p$ has to be investigated separately. We write $F = N_G(D)$ and as in the proof of the previous lemma, we conclude that $G' \leqslant H_GD = H$.

We then assume that $H_G = 1$. From Lemmas 2.2 and 2.8 it follows that $N_G(H) = H \times Z(G)$ and $Z(G) > 1$. Let $z \in Z(G)$ such that $|z| = r$, where r is a prime number. By induction, we have $G' \leqslant N_G(H\langle z \rangle) = L$. If $r \neq q$, we consider the group $E = LN_G(D)$. As E is normal in G, we apply the Frattini argument and thus $G = EN_G(D) = LN_G(D) = E$. Clearly, D is normal in L, hence D is normal in G. As $H_G = 1$, this is not possible. Thus we must have $r = q$ which means that z is a q-element. As D is a Sylow q-subgroup of G, it is clear that $z \in D$. But then $H_G > 1$, a contradiction. The proof is complete.   ☐

Now we are ready to prove

THEOREM 3.4. *Let $p \neq q$ be two prime numbers. If $H \cong (C_{p^k} \times C_p) \times D$, where p is an odd prime, $k \geqslant 2$ and D is an Abelian Sylow q-subgroup of G, then H_G is not trivial.*

PROOF: Again we assume that G is a minimal counterexample, hence $H_G = 1$. We proceed as in the beginning of the proof of Theorem 3.1 and we conclude that there is an element $z \in Z(G)$ such that $|z| = r$, where r is a prime number. We also have

a normal subgroup K of G such that $K > \langle z \rangle$ is the largest normal subgroup of G contained in $H\langle z \rangle$.

Assume first that $r \neq p$. If p divides $|K|$, then K has a nontrivial normal Sylow p-subgroup $P \leqslant H$ and it is clear that P is normal in G. If p does not divide $|K|$, then the Sylow p- subgroup of HK/K is isomorphic to $C_{p^k} \times C_p$ and by Theorem 3.1 or by induction, we conclude that there exists a normal subgroup N of G such that $K < N \leqslant HK = H\langle z \rangle$, a contradiction.

Thus we may assume that $r = p$. If K has a Sylow q-subgroup Q, then $Q \leqslant H$ is normal in G and therefore q does not divide $|K|$. If K contains an element $x \in H$ of order p^l $(l \geqslant 2)$, then $\Phi(K)$ is a nontrivial subgroup of H which is normal in G. As this is not possible, we conclude that K is an elementary Abelian p-group.

If the Sylow p-subgroup of HK/K is cyclic or isomorphic to $C_{p^l} \times C_p$ $(l \geqslant 2)$, then by Lemma 2.7 or by induction there exists a normal subgroup M of G such that $K < M \leqslant HK$. This is not possible and therefore $HK/K \cong (C_p \times C_p) \times D$. We conclude that $k = 2$ and $H = (\langle y \rangle \times \langle x \rangle) \times D$, where $|y| = p^2$ and $|x| = p$. Furthermore, $K = \langle y^p, z \rangle$. By Lemma 3.3, $(G/K)' \leqslant N_{G/K}(HK/K)$, which means that $G' \leqslant N_G(HK)$. Then consider the group $T = N_G(HK)N_G(D)$. As $T \geqslant G'$, it follows that T is normal in G. We use the Frattini argument and see that $G = N_G(HK)N_G(D)$. Since D is normal in $N_G(HK)$, it follows that D is normal in G. But then $H_G > 1$, a contradiction. The proof is complete. ☐

4. Loop theoretical results

In Theorems 3.1 and 3.4 we have two purely group theoretical results which tell us how the structure of an Abelian subgroup with connected transversals determines the subgroup not to be core-free. When we combine Theorem 3.1 with Theorem 2.1 we immediately have the following result in loop theory.

COROLLARY 4.1. *Let p be an odd prime number and Q a finite loop. Then the inner mapping group $I(Q)$ can not be isomorphic to $C_{p^k} \times C_p$, where $k \geqslant 2$.*

Theorem 3.4 also has an interpretation in loop theory.

COROLLARY 4.2. *Let Q be a finite loop and p, q two different prime numbers such that p is odd and q does not divide $|Q|$. Then the inner mapping group $I(Q)$ can not be isomorphic to $(C_{p^k} \times C_p) \times D$, where $k \geqslant 2$ and D is an Abelian q-group.*

PROOF: Suppose the claim is false and we have a finite loop Q whose inner mapping group $I(Q)$ is isomorphic to the Abelian group given in the corollary. Now $M(Q) = AI(Q) = BI(Q)$ and $|A| = |B| = |Q|$ (here A and B denote the sets of left and right translations introduced in the beginning of Section 2). As q does not divide $|Q|$, it follows that D is a Sylow q-subgroup of $M(Q)$. By Theorem 3.4, $I(Q)$

is not core-free in $M(Q)$ contradicting the properties of $I(Q)$ (see the beginning of Section 2). The proof is complete. □

If G is a finite nonabelian group and H is a nontrivial proper subgroup of G, then we consider the following conditions on H: 1) $H_G > 1$, 2) $N_G(H) > HZ(G)$, 3) H is cyclic, 4) $H \cong C_{p^k} \times C_p$, where p is odd and $k \geqslant 2$. From the properties of the inner mapping group of a loop (see Theorems 2.1 and 4.1 and lemmas 2.2 and 2.5) it follows that if each nontrivial proper subgroup of G satisfies at least one of the conditions 1), 2), 3) and 4), then G is not isomorphic to the multiplication group of a loop. We now use these conditions in the following example.

EXAMPLE. Let R be a cyclic group of order r, T a cyclic group of order t and let $\gcd(t, r) = 1$. Assume further that p is an odd prime, $p^k (k \geqslant 2)$ divides $|\text{Aut}(R)|$, p divides $|\text{Aut}(T)|$ and p divides neither r nor t. Now let U be the semidirect product of R and the cyclic group of order p^k and let V be the semidirect product of T and the cyclic group of order p. Then $G = U \times V$ is a finite group of order rtp^{k+1} and $Z(G) = 1$. By looking at the subgroups of this group one sees that each nontrivial proper subgroup satisfies at least one of the four conditions listed before. Thus G is not isomorphic to the multiplication group of a loop.

FINAL REMARKS. In the light of the results given in our corollaries, it is quite natural to ask whether these results hold when $p = 2$. It would also be interesting to prove Corollary 4.2 in the following more general form: $I(Q)$ is not isomorphic to $(C_{p^k} \times C_p) \times D$, where $k \geqslant 2$ and D is a finite Abelian group such that p does not divide $|D|$.

REFERENCES

[1] R. Baer, 'Erweiterung von Gruppen und ihren Isomorphismen', *Math. Z.* **38** (1934), 375–416.

[2] R.H. Bruck, 'Contributions to the theory of loops', *Trans. Amer. Math. Soc.* **60** (1946), 245–354.

[3] J. Denes and A. Keedwell, 'A new authentication scheme based on latin squares', *Discrete Math.* **106/107** (1992), 157–161.

[4] T. Foguel and A. Ungar, 'Gyrogroups and the decomposition of groups into twisted subgroups and subgroups', *Pacific J. Math.* **197** (2001), 1–11.

[5] B. Huppert, *Endliche Gruppen I*, Die Grundlehren der Mathematischen Wissenschaften **134** (Springer-Verlag, Berlin, Heidelberg, New York, 1967).

[6] T. Kepka, 'On the abelian inner permutation groups of loops', *Comm. Algebra.* **26** (1998), 857–861.

[7] T. Kepka and M. Niemenmaa, 'On loops with cyclic inner mapping groups', *Arch. Math.* **60** (1993), 233–236.

[8] C. Moore, D. Therien, F. Lemieux, J. Berman and A. Drisko, 'Circuits and expressions with nonassociative gates', *J. Comput. System Sci.* **60** (2000), 368–394.

[9]   M. Niemenmaa, 'On the structure of the inner mapping groups of loops', *Comm. Algebra* **24** (1996), 135–142.

[10] M. Niemenmaa and T. Kepka, 'On multiplication groups of loops', *J. Algebra* **135** (1990), 112–122.

[11] M. Niemenmaa and T. Kepka, 'On connected transversals to abelian subgroups', *Bull. Austral. Math. Soc.* **49** (1994), 121–128.

[12] H.O. Pflugfelder, 'Historical notes on loop theory', *Comment. Math. Univ. Carolin.* **41** (2000), 359–370.

[13] J.D. Phillips, 'A note on simple groups and simple loops', in *Proceedings of the Groups (Korea 1998)* (Walter de Gruyter, Berlin, New York, 2000), **pp.** 305–317.

[14] J.D.H. Smith, 'Loops and quasigroups: aspects of current work and prospects for the future', *Comment. Math. Univ. Carolin.* **41** (2000), 415–427.

[15] A. Vesanen, 'Solvable loops and groups', *J. Algebra* **180** (1996), 862–876.

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