Comment.Math.Univ.Carolin. 41,4 (2000)687–691

On abelian inner mapping groups of finite loops

Markku Niemenmaa

Abstract. In this paper we consider finite loops of specific order and we show that certain abelian groups are not isomorphic to inner mapping groups of these loops. By using our results we are able to construct a finite solvable group of order 120 which is not isomorphic to the multiplication group of a finite loop.

Keywords: loop, group, connected transversals
Classification: 20D10, 20N05

1. Introduction

We say that a groupoid Q is a loop if Q has unique division and a neutral element (thus loops are nonassociative versions of groups). If Q is a loop, then we have two permutations L_a and R_a on Q defined by $L_a(x) = ax$ and $R_a(x) = xa$ for each $a \in Q$. The permutation group $M(Q) = \langle L_a, R_a : a \in Q\rangle$ is called the multiplication group of Q. By $I(Q)$ we denote the stabilizer of the neutral element of Q and $I(Q)$ is called the inner mapping group of Q. We immediately have two interesting problems here: 1) Which permutation groups are multiplication groups of loops? 2) Which groups are isomorphic to multiplication groups of loops? Some results are known: abelian groups are isomorphic to multiplication groups of loops (this is the trivial case); for every $n \geq 5$ there exists a loop of order n such that $M(Q) = S_n$ (see [1]) and for every $n \geq 6$ there exists a loop of order n such that $M(Q) = A_n$ (see [2]). Liebeck [4] proved that the triality group $D_4(q)$ is isomorphic to the multiplication group of a loop. We also have results in the negative direction: Hamiltonian groups, dihedral groups and nonprimary Redei groups are not isomorphic to multiplication groups of loops (see [6]). Vesanen [9], [10] managed to show that the groups $PSL(2, q)$ are not isomorphic to multiplication groups of loops if $q > 59$ is a power of an odd prime or if $q = 2^n$. When we investigate the structure of $M(Q)$, then it is very useful to see what is happening with the inner mapping group $I(Q)$. It is easy to see that $I(Q) = 1$ if and only if Q is an abelian group. We also know ([3,6]) that $I(Q)$ can neither be cyclic nor the Prüfer group. In [5] we managed to show that if Q is a finite loop, then $I(Q)$ cannot be isomorphic to $C_n \times D$, where C_n is a cyclic group of order $n > 1$, D is an abelian group and $gcd(n, |D|) = 1$. In this paper we consider finite loops Q of specific order and we show that $I(Q)$ cannot be isomorphic to $C_{p^2} \times C_p$, where p is a prime number. The same is true for the groups $E \times D$, where $E \cong C_{p^2} \times C_p$, $D \cong C_q \times C_q$ and $p \neq q$ are prime numbers.

By using the first result we are able to construct a solvable group of order 120 which is not isomorphic to the multiplication group of a loop.

2. Connected transversals

Now we assume that Q is a loop. We write $A = \{L_a : a \in Q\}$ and $B = \{R_a : a \in Q\}$. Then the commutator subgroup $[A, B] \leq I(Q)$ and A and B are left transversals to $I(Q)$ in $M(Q)$. If $1 < K \leq I(Q)$, then K is not a normal subgroup of $M(Q)$. Finally, $M(Q) = \langle A, B \rangle$.

We then consider the situation in groups: 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 $[A, B] \leq H$. In fact, H-connected transversals are both left and right transversals ([6, Lemmas 2.1 and 2.2]). By H_G we denote the core of H in G, i.e. the largest normal subgroup of G contained in H. 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 [6, Theorem 4.1].

In the following lemmas, which are later needed in the proof of our main theorem, we assume that A and B are H-connected transversals. As usual p denotes a prime number.

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 $C \subseteq K_G$.*

For the proofs, see [6, Lemma 2.5 and Proposition 2.7]. 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 $G = \langle A, B \rangle$.

Lemma 2.4. *If H is a cyclic subgroup of G, then $G' \leq H$.*

Lemma 2.5. *If $H \cong C_p \times C_p$, then $G' \leq N_G(H)$.*

Lemma 2.6. *If G is a finite group and $H \cong C_n \times D$, where $n > 1$ and $gcd(n, |D|) = 1$, then $H_G > 1$.*

Lemma 2.7. *If G is a finite group and H is abelian, then H is subnormal in G.*

For the proofs, see [3, Theorem 2.2], [7, Lemma 4.2], [5, Theorem 2.3 and Lemma 2.1].

We still need the following solvability criterion.

Lemma 2.8. *If H is finite and abelian, then G is solvable.*

For the proof, see [7, Theorem 4.1].

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

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

For the proof, see [8, Theorem 5.48].

3. Main theorems

In this section we assume that G is a finite group and H is an abelian subgroup of G with a special structure and with H-connected transversals A and B.

Theorem 3.1. *Let p be a prime number and $|G| = p^n t$, where $gcd(p,t) = 1$ and $3 \leq n \leq 4$. If $G = \langle A, B\rangle$ and $H \cong C_{p^2} \times C_p$, then H_G is not trivial.*

Proof: Let G be a minimal counterexample. Thus $H_G = 1$. We write $H = \langle y\rangle \times \langle x\rangle$, where $|y| = p^2$ and $|x| = p$. From Lemmas 2.2 and 2.7 it follows that $N_G(H) = H \times Z(G)$ and $Z(G) > 1$. If $1 \neq z \in Z(G)$ and $|z| = r \neq p$, where r is a prime number, then we can consider the group $G/\langle z\rangle$ and the subgroup $H\langle z\rangle/\langle z\rangle$. It follows that there exists a normal subgroup N of G such that $\langle z\rangle < N \leq H\langle z\rangle$. Now N contains a nontrivial normal Sylow p-subgroup P, hence P is normal in G and thus $H_G > 1$. The proof is complete in the case that $n = 3$. From now on we assume that $n = 4$ and we may also assume that $Z(G)$ is cyclic of order p.

Then let $z \in Z(G)$ and $|z| = p$. We write $K = N_G(H) = H \times \langle z\rangle$ and $D = K_G$. Clearly, $\langle z\rangle < D \leq K$ and $D \cap H > 1$. Now consider G/D and HD/D. Obviously, HD/D is either cyclic or isomorphic to $C_p \times C_p$. If HD/D is cyclic, then by Lemma 2.4 $(G/D)' \leq HD/D$, hence $G' \leq HD = K$. But then K is normal in G and by Lemma 2.9, $Fr(K) = \langle y^p\rangle$ is normal in G and $H_G > 1$.

Thus we may assume that $HD/D \cong C_p \times C_p$. This means that $D = \langle y^p, z\rangle$. By Lemma 2.5, it follows that $(G/D)' \leq N_{G/D}(HD/D)$ and we conclude that $G' \leq N_G(K)$. Of course, then $N_G(K)$ is normal in G. As $n = 4$, it follows that K is a Sylow p-subgroup of G. Thus K is a characteristic subgroup of $N_G(K)$ and therefore K is normal in G. Again, by Lemma 2.9, $Fr(K) = \langle y^p\rangle$ is normal in G and $H_G > 1$. This completes the proof. □

The following lemma will be needed in the proof of Theorem 3.3. As before, A and B are H-connected transversals. Here we need no restrictions on the order of G.

Lemma 3.2. *Let $G = \langle A, B\rangle$ be a finite group and $H \cong E \times D$, where $E \cong C_p \times C_p$, $D \cong C_q \times C_q$ and $p \neq q$ are prime numbers. Then $G' \leq N_G(H)$.*

Proof: We assume that G is a counterexample of smallest possible order. If $H_G > 1$, then we can use Lemmas 2.4, 2.5 and 2.6 and we conclude that either $G' \leq N_G(H)$ or there exists a normal subgroup N of G such that $H_G < N \leq H$, a contradiction.

Thus we may assume that $H_G = 1$. From Lemmas 2.2 and 2.7 it follows that $N_G(H) = HZ(G)$ and $Z(G) > 1$. If $1 \neq z \in Z(G)$, then by considering the group $G/\langle z\rangle$, we immediately have $G' \leq N_G(H\langle z\rangle)$. Let $L = \cap H\langle z\rangle$, where z goes through all the nontrivial elements of $Z(G)$. If $L = H$, then $G' \leq N_G(H)$.

Thus we continue with the assumption that $L > H$. Of course, this means that $Z(G)$ is a cyclic group of prime power order, say $|Z(G)| = s^n$. We can assume that $s \neq p$.

Let $P \geq E$ be a Sylow p-subgroup of G. If $1 \neq z \in Z(G)$, we write $K = H\langle z\rangle$. Since $G' \leq N_G(K)$, it follows that $N_G(K)$ is normal in G. It is also clear that E is normal in $N_G(K)$. We next consider the group $F = N_G(K)N_G(P)$. As $G' \leq N_G(K) \leq F$, we have that F is normal in G. As P is a Sylow subgroup of F, the Frattini argument gives $G = FN_G(P)$. As $N_G(P) \leq F$, we obtain $G = F$. Now $\langle E^g \mid g \in G\rangle = E^G$ is normal in G and since $G = F$, we conclude that $E^G \leq P$. We consider G/E^G and the subgroup HE^G/E^G which is isomorphic to $C_q \times C_q$. By Lemma 2.5, $(G/E^G)' \leq N_{G/E^G}(HE^G/E^G)$ and so $G' \leq N_G(HE^G)$. Thus $G' \leq N_G(HE^G \cap K) = N_G(H)$. The proof is complete. □

Theorem 3.3. *Let $|G| = p^n t$, where p is a prime number, $gcd(p,t) = 1$ and $3 \leq n \leq 4$. Assume further that $G = \langle A, B\rangle$ and $H \cong E \times D$, where $E \cong C_{p^2} \times C_p$, $D \cong C_q \times C_q$ and $q \neq p$ is a prime number. Then H_G is not trivial.*

Proof: We assume that G is a minimal counterexample and thus $H_G = 1$. It follows from Lemmas 2.2 and 2.7 that $Z(G) > 1$. Let $z \in Z(G)$ and $|z| = r$, where r is a prime number. Assume first that $r \neq p$. Consider $G/\langle z\rangle$ and $H\langle z\rangle/\langle z\rangle$. It follows that there is a normal subgroup N of G such that $\langle z\rangle < N \leq H\langle z\rangle$. Of course, N is the largest normal subgroup of G contained in $H\langle z\rangle$. Thus $|N| = red$, where e divides $|E| = p^3$ and d divides $|D| = q^2$.

If $e > 1$, then N has a Sylow p-subgroup which is contained in H. This Sylow subgroup is normal in G and thus $H_G > 1$.

If $e = 1$, then $|N| = rd$. If $r \neq q$, then the Sylow q-subgroup of N is normal in G and $H_G > 1$. If $r = q$, then consider G/N and HN/N. Now $HN/N \cong E \times C_q$ or $HN/N \cong E$. In both cases we have a normal subgroup M of G such that $N < M \leq HN = H\langle z\rangle$, a contradiction.

Thus we may assume that $r = p$. If $n = 3$, then $z \in E$ and $H_G > 1$. From now on $n = 4$, $d = 1$ and $e > 1$. We conclude that $N \leq E\langle z\rangle$ and $|N|$ divides p^4. If $N = E\langle z\rangle$, then $1 < Fr(N) \leq H$ and $Fr(N)$ is normal in G; therefore we may assume that $N < E\langle z\rangle$.

If EN/N is cyclic, then $HN/N \cong C_n \times D$ (here $n = p^2$ or $n = p$) and we have a contradiction by Lemma 2.6. Thus we suppose that $HN/N \cong (C_p \times C_p) \times D$. If $y \in H$ such that $|y| = p^2$, then $N = \langle y^p, z\rangle$.

By Lemma 3.2, $G' \leq N_G(H\langle z\rangle)$ which means that $N_G(H\langle z\rangle)$ is normal in G. It is clear that D is normal in $N_G(H\langle z\rangle)$. Then let $Q \geq D$ be a Sylow q-subgroup of G. We consider the group $F = N_G(H\langle z\rangle)N_G(Q)$ and as in the proof of Lemma 3.2, we conclude that $D^G \leq Q$. As $HD^G/D^G \cong E$, it follows that there is a normal subgroup L of G such that $D^G < L \leq HD^G$. Now HL/L is cyclic or $HL/L \cong C_p \times C_p$. If HL/L is cyclic, then by Lemma 2.4, $G' \leq HL$ and HL is normal in G. Thus $HL \cap N = \langle y^p\rangle$ is normal in G. If $HL/L \cong C_p \times C_p$, then $L = \langle y^p\rangle D^G$ and $L \cap N = \langle y^p\rangle$ is again normal in G, hence $H_G > 1$. This completes the proof. □

After having proved our purely group theoretical results we can return to consider the structure of finite loops and their inner mapping groups and multiplication groups. By combining Theorems 2.1, 3.1 and 3.3, we get

Theorem 3.4. *Let p be a prime number and let Q be a finite loop such that $|Q| = t$ or $|Q| = pt$, where $gcd(p,t) = 1$. Then $I(Q) \cong E$ or $I(Q) \cong E \times D$, where E and D are as in Theorem 3.3, is not possible.*

Then let G be a finite group and let H be a nontrivial proper subgroup of G. We consider the following four conditions on H: 1) $H_G > 1$, 2) $N_G(H) > HZ(G)$, 3) H is cyclic, 4) $H \cong C_{p^2} \times C_p$, where p is a prime number and p does not divide $[G : H]$. If each proper nontrivial subgroup of G satisfies either 1), 2), 3) or 4), then G is not isomorphic to the multiplication group of a loop. We now introduce an example, where we can apply this approach.

Example. *Let $G = H \times K$, where $H = Hol(C_5)$ (the holomorph of the cyclic group C_5) and $K = S_3$ (the symmetric group of degree 3). Now $|G| = 120$ and if G is the multiplication group of a loop Q, then clearly $|Q| \geq 5$. Thus we may concentrate on the properties of those subgroups of G, whose order ≤ 24. It is very easy to go through the cyclic subgroups of G and for the rest we can apply either 1) or 2) with one exception: G has a subgroup $H \cong C_4 \times C_2$ with $H_G = 1$ and $N_G(H) = HZ(G) = H$. However, by applying condition 4), we see that H cannot be in the role of $I(Q)$. It follows that G cannot be isomorphic to the multiplication group of a loop.*

References

[1] Denes J., Keedwell A.D., *Latin squares and their applications*, Akademiai Kiado, Budapest, 1974.

[2] Drápal A., Kepka T., *Alternating groups and latin squares*, European J. Combin. **10** (1989), 175–180.

[3] Kepka T., Niemenmaa M., *On loops with cyclic inner mapping groups*, Arch. Math. **60** (1993), 233–236.

[4] Liebeck M., *The classification of the finite simple Moufang loops*, Math. Proc. Camb. Phil. Soc. **102** (1987), 33–47.

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

[6] Niemenmaa M., Kepka T., *On multiplication groups of loops*, J. Algebra **135** (1990), 112–122.

[7] Niemenmaa M., Kepka T., *On connected transversals to abelian subgroups*, Bull. Austral. Math. Soc. **49** (1994), 121–128.

[8] Rotman J., *An introduction to the theory of groups*, Springer-Verlag, 1995.

[9] Vesanen A., *On connected transversals in $PSL(2,q)$*, Ann. Acad. Sci. Fenn., Series A, I. Mathematica, Dissertationes 84, 1992.

[10] Vesanen A., *The group $PSL(2,q)$ is not the multiplication group of a loop*, Comm. Algebra **22** (1994), 1177–1195.

Department of Mathematical Sciences, University of Oulu, Finland

(*Received* September 3, 1999)