BULL. AUSTRAL. MATH. SOC. 20N05
VOL. 38 (1988) [171–176]

ON CONJUGACY CLASSES IN FINITE LOOPS

T. KEPKA AND M. NIEMENMAA

The rôle of the conjugacy relation is certainly important in the structure theory of groups. Here we study this relation in a considerably more general setting, namely in the theory of loops. We first recall some basic facts about quasigroups, their multiplication groups, their inner mapping groups and the conjugacy relation. After this we estimate the size and the number of the conjugacy classes and we study the structure of loops having only two conjugacy classes. Finally, the values of the centraliser function are discussed.

1. PRELIMINARIES

Let Q be a finite loop (that is a finite groupoid with unique division and an identity element usually denoted by e). For every $a \in Q$, the left translation L_a and the right translation R_a are permutations on Q defined by: $L_a(x) = ax$ and $R_a(x) = xa$ for every $x \in Q$. The set of all left and right translations generates a subgroup $M(Q)$ of $S(Q)$ (the group of all permutations on Q). We say that $M(Q)$ is the *multiplication group* of Q. Clearly, $M(Q)$ is transitive on Q and the stabilisers of elements of Q are conjugate in $M(Q)$. We denote by $I(Q)$ the stabiliser of the indentity element e; thus $I(Q) = \{P \in M(Q): P(e) = e\}$. This permutation group is called the *inner mapping group* of Q. Now $\operatorname{card}(M(Q)) = \operatorname{card}(Q) \cdot \operatorname{card}(I(Q))$.

Recall that the *left*, *right* and *middle nucleus* of Q are defined as follows:

$$N_l(Q) = \{a \in Q: a \cdot xy = ax \cdot y \text{ for all } x, y \in Q\};$$
$$N_r(Q) = \{a \in Q: xy \cdot a = x \cdot ya \text{ for all } x, y \in Q\};$$
$$N_m(Q) = \{a \in Q: xa \cdot y = x \cdot ay \text{ for all } x, y \in Q\}.$$

Further, $N(Q) = N_l(Q) \cap N_r(Q) \cap N_m(Q)$ is called the *nucleus* of Q and $C(Q) = \{a \in N(Q): L_a = R_a\}$ is the *centre* of Q. All the nuclei are subloops of Q and the centre is an abelian subgroup. We characterise the centre by

LEMMA 1.1. $C(Q) = \{a \in Q: I(Q)(a) = a\} = \{a \in Q: L_a \in Z(M(Q))\} = \{a \in Q: R_a \in Z(M(Q))\}$

For proof, see [3, pp. 60–62] and [8, pp. 217–218].

Received 28 October, 1987

From Lemma 1.1 it follows that the groups $C(Q)$ and $Z(M(Q))$ are isomorphic. It is also very easy to see that $I(Q) = \{1\}$ if and only if Q is an abelian group.

Now $I(Q)$ is a permutation group on Q and this means that its orbits determine an equivalence relation α on Q. If $(a,b) \in \alpha$, then we say that the elements a and b are *conjugate* in Q. For any $a \in Q$, $I(Q)(a)$ is the set of elements conjugate to a. By Lemma 1.1, every element of $C(Q)$ forms a one-element class of α. Clearly, $\operatorname{card}(I(Q)(a))$ divides $\operatorname{card}(I(Q))$ for every $a \in Q$.

THEOREM 1.1. *Suppose that Q is not an abelian group. Then the factor loop $Q/C(Q)$ contains at least three elements.*

PROOF: Put $S = Q/C(Q)$. If $\operatorname{card}(S) = 1$, then $Q = C(Q)$, a contradiction. Next assume that $\operatorname{card}(S) = 2$. It follows that there is an element $a \in Q$ such that $Q = C(Q) \cup aC(Q)$, $C(Q) \cap aC(Q) = \emptyset$. Let x, $y \in C(Q)$. Now $ax \cdot ay = a^2 \cdot xy$, $a(ax \cdot ay) = (a \cdot a^2)(xy) = (a^2 \cdot a)(xy) = a^2(a \cdot xy) = a^2(ax \cdot y) = a^2(xa \cdot y) = a^2(x \cdot ay) = a^2x \cdot ay = (a \cdot ax)(ay)$. We conclude that $a \in N_l(Q)$. In a similar way we can show that $a \in N_r(Q)$, $a \in N_m(Q)$ and, finally, $a \in C(Q)$. But then $C(Q) = aC(Q)$, a contradiction. Thus $\operatorname{card}(S) \geqslant 3$. ∎

Now let $n = \operatorname{card}(Q)$, $r =$ the number of conjugacy classes and $m = \operatorname{card}(C(Q))$. We have

LEMMA 1.2. *If Q is an abelian group, then $m = r = n$. If Q is not an abelian group, then $n \geqslant 5$, $2 \leqslant r \leqslant 2n/3$ and $1 \leqslant m \leqslant n/3$.*

PROOF: If $n \in \{1,2,3,4\}$ then Q is abelian group. If Q is not an abelian group, then $n \geqslant 5$ and $r \geqslant 2$. By Theorem 1.1, $m \leqslant n/3$ and since $r - m \leqslant (n-m)/2$, it follows that $r \leqslant 2n/3$. ∎

For basic facts about groups and loops we refer to [7] and [3].

2. BOUNDS FOR THE NUMBER OF CONJUGACY CLASSES

Let Q be a loop of order n. A subset M of Q is said to be *tame* if there exists $P \in I(Q)$ $(P \neq 1)$ Such that $P(x) = x$ for every $x \in M$. Now we define

$$t(Q) = \max\{\operatorname{card}(M) : M \text{ is tame}\} \text{ and}$$
$$t(Q) = 0, \qquad \text{if } I(Q) = \{1\}.$$

We know already that $I(Q) = \{1\}$ if and only if Q is an abelian group. If Q is a nonabelian group, then $t(Q) = \max\{\operatorname{card}(C_Q(x)) : x \in Q - Z(Q)\}$. This means that we are dealing with large centralisers and we shall return to this topic in section four. Now we shall use $t(Q)$ in order to estimate m and r.

https://doi.org/10.1017/S000497270002743X Published online by Cambridge University Press

LEMMA 2.1. *If Q is not an abelian group, then $t(Q) \geqslant 2m$.*

PROOF: Suppose that Q is not commutative. Then $L_a \neq R_a$ for some $a \in Q$ and $1 \neq P = R_a^{-1}L_a \in I(Q)$. Clearly, $a \notin C(Q)$ and $P(x) = x$ for every $x \in C(Q) \cup aC(Q)$. It follows that $t(Q) \geqslant 2m$.

Now we assume that Q is commutative. Since Q is not associative we can find a permutation S such that $1 \neq S = L_a^{-1}L_b^{-1}L_{ba} \in I(Q)$. Here $b \notin C(Q)$ and for any $c \in C(Q)$ we have

$$ba \cdot bc = (ba \cdot b)c = (b \cdot ab)c = b(ab \cdot c) = b(a \cdot bc),$$

and so $S(bc) = bc$. But then $S(x) = x$ for every $x \in C(Q) \cup bC(Q)$ and again $t(Q) \geqslant 2m$. The proof is complete. ∎

Now assume that Q is not an abelian group (and hence $n \geqslant 5$). Let $Q_1, \ldots, Q_r$ be the conjugacy classes and $n_1 = \operatorname{card}(Q_1) \leqslant n_2 = \operatorname{card}(Q_2) \leqslant \cdots \leqslant n_r = \operatorname{card}(Q_r)$. Then $1 \leqslant m < r$, $n_1 = \cdots = n_m = 1$ and $2 \leqslant n_i$, $i = m+1, \ldots, r$. We next establish

THEOREM 2.1. *Let $m+1 \leqslant j \leqslant r$. Then $n \leqslant t(Q)n_j$.*

PROOF: Assume by way of contradiction that $n > t(Q)n_j$ for some j ($m+1 \leqslant j \leqslant r$). Now $P_x = R_x^{-1}L_x \in I(Q)$ for every $x \in Q$. We shall first prove that $P_a = 1$ for every $a \in Q_j$. If $a \in Q_j$, then $P_x(a) \in Q_j$ for every $x \in Q$. For every $b \in Q_j$ we define the set

$$A_b = \{x \in Q : P_x(a) = b\}.$$

Now $n = \sum_{b \in Q_j} \operatorname{card}(A_b) > t(Q)n_j$, hence $\operatorname{card}(A_b) > t(Q)$ for some $b \in Q_j$. Clearly, $L_b^{-1}R_a(x) = x$ for every $x \in A_b$. Furthermore, if $c \in A_b$, then $S = L_c^{-1}L_b^{-1}R_aL_c \in I(Q)$ and $S(x) = x$ for every $x \in L_c^{-1}(A_b)$. Since $\operatorname{card}\left(L_c^{-1}(A_b)\right) > t(Q)$, we conclude that $S = 1$ and thus $cy \cdot a = b \cdot cy$ for any $y \in Q$. But then $za = bz$ for every $z \in Q$, $a = b$ and hence $P_a = 1$.

Next we prove that $Q_j \subseteq N_r(Q)$. Let $a \in Q_j$ and $u \in Q$. For every $x \in Q$, $D_x = L_u^{-1}L_x^{-1}L_{xu} \in I(Q)$ and $D_x(a) \in Q_j$. For every $b \in Q_j$, let

$$B_b = \{x \in Q : D_x(a) = b\}.$$

As in the first part of the proof we can again find $b \in Q_j$ such that $\operatorname{card}(B_b) > t(Q)$. Now $R_u^{-1}R_a^{-1}R_{ub}(x) = x$ for every $x \in B_b$ and if $c \in B_b$, then $L_c^{-1}R_u^{-1}R_a^{-1}R_{ub}L_c = 1$. It follows that $cy \cdot ub = (cy \cdot u)a$ for every $y \in Q$. Thus $z \cdot ub = zu \cdot a$ for every u, $z \in Q$, and $a = b$, and consequently $a \in N_r(Q)$.

Likewise it follows that $Q_j \subseteq N_l(Q)$. But then $Q_j \subset C(Q)$, $n_j = 1$ and $j \leqslant m$, a contradiction. ∎

https://doi.org/10.1017/S000497270002743X Published online by Cambridge University Press

THEOREM 2.2. *The following inequalities hold:*

(i) $t(Q) \geqslant (r-m)n/(n-m)$,
(ii) $t(Q) \geqslant (3r-n)/2$,
(iii) $t(Q) \geqslant r-m+1$.

PROOF:

(i) This follows directly from Theorem 2.1.
(ii) By Lemma 1.2, $m \leqslant n/3$ and since $(r-m)/(n-m) \geqslant (r-n/3)/(n-n/3)$, it follows by (i) that $t(Q) \geqslant (r-n/3)n/(n-n/3) = (3r-n)/2$.
(iii) Now $(r-m)n/(n-m) = (r-m)(n-m+m)/(n-m) = r-m+k$, where $k > 0$. ∎

We shall illustrate the situation by some examples.

Example 2.1. For every $n \geqslant 5$ there exists a loop Q of order n such that $M(Q) = S(Q)$ (see [**5**, Theorem 3.1.1.]). Now $m = 1$, $r = 2$ and $t(Q) = n-2$.

Example 2.2. For every $n \geqslant 6$ there exists a loop Q of order n such that $M(Q) = A(Q)$ (the alternating group). Here $m = 1$, $r = 2$ and $t(Q) = n-3$ (for details, see [**6**]).

Example 2.3. Consider a loop Q with the following multiplication table:

1	2	3	4	5	6
2	1	4	3	6	5
3	4	5	6	2	1
4	3	6	5	1	2
5	6	1	2	3	4
6	5	2	1	4	3

Here $m = 2$, $r = 4$ and $t(Q) = 4$. Furthermore, $I(Q)$ is isomorphic to Klein's four group. The factor loop $Q/C(Q)$ is a group of order three.

Remark. If Q is a group of order n, then the number of conjugacy classes has a lower bound, namely $r \geqslant \log(\log n)/\log 2$ (see [**9**]).

3. LOOPS WITH $t(Q) = 2$

Let Q be a loop of order n which is not an abelian group (hence $n \geqslant 5$). In this section we also assume that $t(Q) = 2$. By Theorem 2.2 (iii), $r \leqslant t(Q) + m - 1 = m+1$ and obviously $r = m+1$. By Lemma 2.1, $2 = t(Q) \geqslant 2m \geqslant m+1 = r$ which gives $r = 2$ and $m = 1$.

https://doi.org/10.1017/S000497270002743X Published online by Cambridge University Press

Now we can consider $I(Q)$ as a permutation group on $E = Q - \{e\}$. Clearly, $I(Q)$ is transitive on E and $M(Q)$ is 2-transitive on Q. Furthermore, $I(Q)$ is a Frobenius group and therefore $\operatorname{card}(I(Q)) = k(n-1)$, where k divides $n-2$.

THEOREM 3.1. *If $t(Q) = 2$, then Q is simple and Q is either commutative or anticommutative (that is $ab \neq ba$ whenever $e \neq a \neq b \neq e$).*

PROOF: Since $M(Q)$ is 2-transitive it is primitive and it follows that Q is simple (see [**10**, p. 10]).

Suppose then that $ab = ba$ for some $e \neq a \neq b \neq e$. Put $P = R_a^{-1}L_a$, then $P(e) = e$, $P(a) = a$ and $P(b) = b$. Since $t(Q) = 2$, we conclude that $P = 1$. Consequently, $ax = xa$ for every $x \in Q$. Hence, if $S = R_x^{-1}L_x$ $(x \neq e,\ x \neq a)$, then $S(e) = e$, $S(a) = a$ and $S(x) = x$ and necessarily $S = 1$. But then $xy = yx$ for every $x, y \in Q$. ∎

THEOREM 3.2. *Let Q be a loop which is not an abelian group and let $t(Q) = 2$. Further, let Q be of the smallest possible order. Then:*

(i) *if A is a subloop of Q $(1 \neq A \neq Q)$, then A is a group of order two;*
(ii) $n \geqslant 6$.

PROOF:

(i) If A is not an abelian group then A satisfies $t(A) = 2$, too. This is a contradiction, hence A is an abelian group. Assume now that $\operatorname{card}(A) \geqslant 3$. By Theorem 3.1, Q is commutative. Consider a permutation $P = L_b^{-1}L_a^{-1}L_{ab}$, where $a, b \in A$. It is easy to see that, in fact, $P = 1$ and thus $a \cdot bx = ab \cdot x$ for every $x \in Q$. Similarly, if $S = R_b^{-1}R_x^{-1}R_{bx}$, where $b \in A$ and $x \in Q$, we conclude that $S = 1$. Thus, $y \cdot bx = yb \cdot x$ for every $x, y \in Q$. Finally, if we put $U = R_x^{-1}L_y^{-1}R_xL_y$, then $U = 1$ and we have shown that $y \cdot zx = yz \cdot x$ for every $x, y, z \in Q$. But then Q is an abelian group, a contradiction.

(ii) Let $n = 5$. Now $\operatorname{card}(I(Q))$ is either $= 4$ or $= 12$. Since $t(Q) = 2$, it follows that $\operatorname{card}(I(Q)) = 12$, and so $\operatorname{card}(M(Q)) = 60$. This means that $M(Q)$ is the alternating group on Q. Now the complete list of non-associative loops of order five (see for example [**5**]) reveals the fact that any such loop generates at least one odd permutation, a contradiction. ∎

It seems to be an open problem (at least to the authors) whether there exist loops Q satisfying $t(Q) = 2$.

4. THE CENTRALISER FUNCTION

For $n \geqslant 5$, we define the centraliser function T by $T(n) = \min\{t(Q) :$ Q is a loop of order n which is not an abelian group$\}$. Similarly, for $n \geqslant 1$, put $t(n) =$

https://doi.org/10.1017/S000497270002743X Published online by Cambridge University Press

$\min\{t(G)\colon G$ is a nonabelian group of order $n\}$ and $t(n) = 0$ if all groups of order n are abelian. Clearly, $T(n) \geqslant 2$ and $T(n) \leqslant t(n)$ provided $t(n) \neq 0$. Further $T(5) = 3$ and $t(n) = 0$ if and only if n is cube-free and $(n, \varphi(n)) = 1$; we denote by $\mathcal{A}$ the set of all such integers n.

While nothing is known about $T(n)$ we are able to give a lower bound for $t(n)$. Recall that $t(G) = \max\{\text{card}\,(C_G(x))\colon x \in G - Z(G)\}$.

THEOREM 4.1. *Let $n \geqslant 6$, $n \notin \mathcal{A}$. Then $t(n) > n^{1/4}$. Moreover, $t(n) > n^{1/2}$ provided that n is odd.*

PROOF: Let G be a nonabelian group of order n. If G is soluble, then $t(G) > n^{1/2}$ (see [4]), hence $t(n) > n^{1/2}$ for n odd. Thus we may assume that G is not soluble, hence (by the odd order theorem) n is even. If $Z(G/Z(G)) \neq \{1\}$, then $t(G) > n^{1/2}$ (see [1, Lemma 2]). If $Z(G) = \{1\}$, then we can use the theorem by Brauer and Fowler (see [2]) and $t(G) > n^{1/3}$. Finally, we assume that $Z(G) \neq \{1\}$ and $Z(G/Z(G)) = \{1\}$. Now $H = G/Z(G)$ is of even order k and hence we have an element $aZ(G) \in H$ such that $\text{card}\,(C_H(aZ(G))) > k^{1/3}$ and also $\text{card}\,(C_G(a)) > k^{1/3}$ (see [1, Lemma 1]). It follows that $t(G) > \max\{k^{1/3}, n/k\}$, hence $t(G) > n^{1/4}$. We conclude that $t(n) > n^{1/4}$. This completes the proof. ∎

REFERENCES

[1] E.A. Bertram, 'Large centralizers in finite soluble groups', *Israel J. Math.* **47** (1984), 335–344.

[2] R. Brauer and K. Fowler, 'On groups of even order', *Ann. Math.* **62** (1955), 565–583.

[3] R. Bruck, *A Survey of Binary Systems* (Springer-Verlag, Berlin—Heidelberg—New York, 1971).

[4] J. Cossey, 'Finite soluble groups have large centralizers', *Bull. Austral. Math. Soc.* **35** (1987), 291–298.

[5] J. Dénes and A.D. Keedwell, *Latin Squares and Their Applications* (Akadémiai Kiadó, Budapest, 1976).

[6] A. Drápal and T. Kepka, 'Alternating groups and latin squares' (to appear).

[7] B. Huppert, *Endliche Gruppen I* (Springer-Verlag, Berlin—Heidelberg—New York, 1967).

[8] T. Ihringer, 'Quasigroups, loops and centralizer rings', in *Contributions to General Algebra 3.: Proceedings of the Vienna Conference*, pp. 211–224, 1984.

[9] M. Newman, 'A bound for the number of conjugacy classes in a group', *J. London Math. Soc.* **43** (1968), 108–110.

[10] J.D.H. Smith, *Multiplication Groups of Quasigroups*, Preprint 603, Darmstadt, 1981.

Dr T. Kepka
Charles University
Prague
Czechoslovakia

Dr M. Niemenmaa
Department of Mathematics
University of Oulu
Linnanmaa
90570 Oulu
Finland