Simple quasigroups whose inner permutations commute

T. Kepka, K.K. Ščukin

Abstract. Simple quasigroups with commuting inner permutations are medial.

Keywords: quasigroup, inner permutation
Classification: 20N05

Inner permutation groups of medial quasigroups are two-generated abelian groups and, conversely, quasigroups with at most two-element inner permutation groups are medial (see [2] and [3]). On the other hand, there exist many non-medial quasigroups possessing three-element inner permutation groups (see [4]) and the inner permutation groups of non-commutative eight-element groups are four-element groups (and hence two-generated abelian groups). We show in this short note that a simple quasigroup is medial, provided that the inner permutation group is abelian.

1. Preliminaries.

Let G be a group. Then $[a,b] = a^{-1}b^{-1}ab$ for all $a,b \in G$ and $[A,B] = \{[a,b]; a \in A, b \in B\}$ for subsets A,B of G.

Let H be a subgroup of G. Then $C_G(H)$, $N_G(H)$ and $L_G(H)$ denote the centralizer, the normalizer and the core of H in G, respectively.

The following lemma is obvious:

Lemma 1.1. *Let H be an abelian subgroup of a group G such that $N_G(H) = H$. If $x \in G$ and $N_G(T) \subseteq H$, where $T = H \cap x^{-1}Hx$, then $x \in H$ and $T = H$.*

A quasigroup satisfying the equation $xa \cdot by = xb \cdot ay$ is called medial.

The following result is well known:

Lemma 1.2. *A quasigroup Q is medial iff there exist an abelian group $Q(+)$, commuting automorphisms f,g of $Q(+)$ and an element $a \in Q$ such that $xy = f(x) + g(y) + a$ for all $x,y \in Q$.*

2. Auxiliary results.

In this section, let G be a group such that $G = KH$, where both K and H are abelian subgroups of G, $H \neq G$, $K \neq 1$ and K is normal in G.

The following four lemmas are obvious:

Lemma 2.1. (i) *$H \cap K \subseteq H \cap C_G(K) = H \cap Z(G) \subseteq L_G(H)$.*
(ii) *$Z(G) = (K \cap Z(G))(H \cap Z(G))$.*
(iii) *If $L_G(H) = 1$, then $H \cap K = 1 = H \cap C_G(K)$ and $Z(G) \subseteq K$.*
(iv) *If $Z(G) = 1$, then $H \cap K = 1 = H \cap C_G(K)$.*
(v) *If $H \cap K = 1$, then $L_G(H) = H \cap C_G(K) = H \cap Z(G)$.*

Lemma 2.2. (i) *If E is a subgroup of G such that $H \subseteq E \subseteq G$, then $E = (E \cap K)H$ and $E \cap K$ is normal in G.*

(ii) *If no non-trivial proper subgroup of K is normal in G, then $H \cap K = 1$ and H is maximal in G.*

Lemma 2.3. *Suppose that H is a maximal subgroup of G.*

(i) *If L is a subgroup of K and L is normal in G, then either $L \subseteq H \cap K$ or $K = (H \cap K)L$.*
(ii) *If $H \cap K = 1$, then no non-trivial proper subgroup of K is normal in G.*
(iii) *If H is not normal in G, then $Z(G) \subseteq L_G(H)$.*

Lemma 2.4. *the following conditions are equivalent:*

(i) *H is maximal in G and $H \cap K = 1$.*
(ii) *No non-trivial proper subgroup of K is normal in G.*

In the remaining part of this section, we shall assume that the equivalent conditions of 2.4 are satisfied. By 2.1 (v), $L_G(H) = H \cap C_G(K) = H \cap Z(G)$. If H is not normal in G, then $Z(G) \subseteq H$ and $L_G(H) = Z(G)$. If H is normal in G, then $G \cong K \times H$ is abelian and K is cyclic of prime order.

For every $u \in H$, the mapping $q_u : a \to a^u = u^{-1}au$ is an automorphism of K. Now, we denote by F the subring generated by all these q_u in the endomorphism ring of K and we put $q = -1_F \in F$; we have $q(a) = a^{-1}$ for every $a \in K$ and $q^2 = 1_F = \mathrm{id}_K$.

Lemma 2.5. (i) *F is a field and the dimension of K as a vector space over F is 1; in particular, the groups K and $F(+)$ are isomorphic.*

(ii) *If H is finitely generated, then F and K are finite. If, moreover, $L_G(H) = 1$, then H is finite and cyclic and G is finite.*

Proof: (i) Since H is abelian, F is a commutative ring. If $f \in F$, $f \neq 0_F$, then both $f(K)$ and $\mathrm{Ker}(f)$ are subgroups of K and they are normal in G, and hence $f(K) = K$ and $\mathrm{Ker}(f) = 1$, i.e. f is an automorphism of K.

Now, let $a \in K$, $a \neq 1$. Then $F(a)$ is a subgroup of K (use the fact that $q \in F$) and $F(a)$ is normal in G. Since $a \in F(a)$, we have $F(a) = K$. If $f \in F$, $f \neq 0_F$, then $f^{-1}(a) = g(a)$ for some $g \in F$, $a = fg(a)$ and the equality $F(a) = K$ yields $fg = \mathrm{id}_K = 1_F$. Consequently, $f^{-1} = g \in F$.

(ii) As is well known, any field, finitely generated as a ring, is finite. Now, if $L_G(H) = 1$, then the mapping $u \to q_u^{-1}$ is an injective homomorphism of H into the multiplicative group F^* of non-zero elements of F. However, this group is cyclic. □

Lemma 2.6. *Let A be a subset of G such that $G = AH$ and $[A, A] = 1$. Then:*

(i) *$A \subseteq KL$, $L = L_G(H)$.*
(ii) *If $L = 1$, then $A = K$.*

Proof: There is a uniquely determined subset S of $K\times H$ such that $A=\{au;(a,u)\in S\}$. Further, fix an element $r\in K$, $r\neq 1$. For every $a\in K$, there is a unique $p_a\in F$ with $a=p_a(r)$; we have $p_a\neq 0_F$ iff $a\neq 1$.

Now, assume that there exists a pair $(b,u)\in S$ such that $b\neq 1$ and $u\notin L$. Put $p=(q+q_u^{-1})p_b^{-1}\in F$. Since $u\notin L=H\cap C_G(K)$, we have $u\notin C_G(K)$ and $q+q_u^{-1}\neq 0_F$. Thus $p\neq 0_F$ and there exists $e\in K$ with $e\neq 1$ and $e^{-1}=p^{-1}(r)$. Now, $p_e(r)=e=p^{-1}(r)^{-1}=p^{-1}(r^{-1})=p^{-1}q(r)$, and so $p_e=p^{-1}q$ and $p_e^{-1}=q^{-1}p=qp$. On the other hand, $G=AH$, and hence $(e,v)\in S$ for some $v\in H$. The equality $[A,A]=1$ implies $bueu^{-1}uv=buev=evbu=evbv^{-1}uv$ and $bueu^{-1}=evbv^{-1}$. From this, $(q+q_v^{-1})p_b(r)=b^{-1}vbv^{-1}=e^{-1}ueu^{-1}=(q+q_u^{-1})p_e(r)$ and $(q+q_v^{-1})p_b=(q+q_u^{-1})p_e$, $p=(q+q_u^{-1})p_b^{-1}=(q+q_v^{-1})p_e^{-1}=(q+q_v^{-1})qp$, $1_F=(q+q_v^{-1})q=1_F+q_v^{-1}q$ and $0_F=q_v^{-1}q$, a contradiction.

We have proved that $A\subseteq H\cup KL$. However, if $w\in A\cap H$ and $c\in K$, then $cz\in A$ for some $z\in H$ and $wcz=czw=cwz$, $wc=cw$ and $w\in L\subseteq KL$. Thus $A\subseteq KL$ and the rest is clear. □

Lemma 2.7. (i) $G'\subseteq K$.
(ii) *If H is not normal in G, then $G'=K$.*

Proof: (i) $G/K=H$.

(ii) Since H is not normal in G, we must have $G'\neq 1$. But G' is normal in G and $G'\subseteq K$. □

Corollary 2.8. *Suppose that $L_G(H)=1\neq H$. If A is a subset of G such that $G=AH$ and $[A,A]=1$, then $A=G'$.*

3. Connected transversals to maximal abelian subgroups.

Throughout this section, let H be a proper maximal subgroup of a group G such that H is abelian and not normal in G. Further, let A,B be subsets of G such that $G=AH=BH$ and $[A,B]\subseteq H$.

Lemma 3.1. (i) *$N_G(H)=H$ and $Z(G)\subseteq L_G(H)\neq H$.*
(ii) *If T is a subgroup of H such that $N_G(T)\nsubseteq H$, then $T\subseteq Z(G)$.*

Proof: Obvious. □

Lemma 3.2. (i) *$A\cap H\subseteq L_G(H)$ and $B\cap H\subseteq L_G(H)$.*
(ii) *If $L_G(H)=1$, then $A\cap H=\{1\}=B\cap H$.*

Proof: Easy. □

Lemma 3.3. (i) *$AL_G(H)=BL_G(H)$ is a subgroup of G.*
(ii) *If $L_G(H)=1$, then $A=B$ is an abelian subgroup of G.*

Proof: We can assume without loss of generality that $L_G(H)=1$ (consider the factor group $G/L_G(H)$).

First, let $a\in A$. Then $b^{-1}a\in H$ for some $b\in B$, and hence $b^{-1}a\in H\cap aHb^{-1}=H\cap bHb^{-1}=T$. If $N_G(T)\subseteq H$, then $b\in H$ by 1.1, and so $a=b=1$ by 3.2 (ii).

If $N_G(T) \nsubseteq H$, then $T = 1$ by 3.1 (ii), and so $a = b$. We have proved that $A \subseteq B$. Similarly, $B \subseteq A$ and we get $A = B$.

Now, let $a, b \in A$. Then $c^{-1}ab \in H$ for some $c \in A$ and $c^{-1}ab \in H \cap aHa^{-1} = T$. Again, if $N_G(T) \subseteq H$, then $a \in H$, $a = 1$ and $c = b = ab$. If $N_G(T) \nsubseteq H$, then $T = 1$, $c^{-1}ab = 1$ and $c = ab$. We have proved that $AA \subseteq A$. Similarly, $A^{-1}A \subseteq A$ and $AA^{-1} \subseteq A$. This shows that A is a subgroup of G. Finally, $[A, A] \subseteq A \cap H = 1$ and we see that A is abelian. □

Proposition 3.4. *If $L_G(H) = 1$, then $A = B = G'$ is a normal abelian subgroup of G.*

PROOF: By 3.3 (ii), A is an abelian subgroup of G and consequently $G'' = 1$ by [1]. Since H is not normal in G, we have $G' \nsubseteq H$ and $G = HG'$. Now, $A = G'$ by 2.9. □

Corollary 3.5. *$G''' = 1$ and $AL_G(H) = BL_G(H) = G'L_G(H)$ is a normal subgroup of G.*

Proposition 3.6. *If H is finitely generated, then $G/L_G(H)$ is finite.*

PROOF: See 2.5 (ii) and the proof of 3.4. □

4. Quasigroups with commuting inner permutations.

In this section, let Q be a non-trivial quasigroup. If $a \in Q$, then we can define permutations $L(a)$ and $R(a)$ of Q by $L(a)(x) = ax$ and $R(a)(x) = xa$ for every $x \in Q$. The permutation group $M(Q)$ generated by all these $L(a)$ and $R(a)$, $a \in Q$, is called the multiplication group of Q. The stabilizer $I(Q, a) \subseteq M(Q)$ of $a \in Q$ is called the inner permutation group (with respect to a). Since $M(Q)$ is transitive, the inner permutation groups are conjugate, and hence isomorphic.

The following lemma is well known and easy.

Lemma 4.1. *The following conditions are equivalent:*

(i) *Q is c-simple, i.e. id_Q and $Q \times Q$ are the only cancellative congruences of Q.*
(ii) *$M(Q)$ is a primitive permutation group on Q.*
(iii) *$I(Q, a)$ is a maximal subgroup of $M(Q)$ for at least one (and then for every) $a \in Q$.*

Theorem 4.2. *Suppose that Q is c-simple and that the inner permutation group $I(Q, a)$ is abelian. Then Q is a finite medial quasigroup.*

PROOF: Let $a, b \in Q$ be such that $a = ba$. Put $G = M(Q)$, $H = I(Q, a)$, $A = \{R(x)R(a)^{-1}; x \in Q\}$ and $B = \{L(x)L(b)^{-1}; x \in Q\}$. Then H is a proper maximal subgroup of G, H is abelian, $L_G(H) = 1$, $G = AH = BH$ and $[A, B] \subseteq H$. If H is normal in G, then $H = 1$ and $G = Q$ is a cyclic group of prime order. Hence, assume that H is not normal in G. By 3.4, $A = B = G'$ is a normal abelian subgroup of G.

Now, define a binary operation $+$ on Q by $x + y = f^{-1}(x)g^{-1}(y)$ where $f = R(a)$ and $g = L(b)$. Then $Q(+)$ is a loop and $a = 0$, i.e. a is the neutral element of $Q(+)$. Moreover, $xy = f(x) + g(y)$, $L(x, +) = L(f^{-1}(x))g^{-1}$ and $R(y, +) = R(g^{-1}(y))f^{-1}$. From this, it is easy to see that $M(Q(+)) = A = B = G'$. In particular, $M(Q(+))$

is an abelian group, and hence $Q(+) = M(Q(+))$ is also an abelian group. Further, put $c = aa$ and $f_1 = R(c,+)^{-1}f$. Then $f_1(a) = a$, $f_1 \in H$ and $f(x) = f_1(x) + c$. Similarly, if $g_1 = R(a,+)^{-1}g$, then $g_1 \in H$ and $g(y) = g_1(y) + a$. Now, $xy = f_1(x) + g_1(y) + d$, $d = a + c$. Since $f_1, g_1 \in H$, we have $f_1g_1 = g_1f_1$. If $h \in H$ and $u \in Q$, then $hL(u,+)h^{-1} = L(v,+)$ for some $v \in Q$ and $h(u+x) = v + h(x)$ for every $x \in Q$. In particular, $h(u) = h(u+0) = v + h(0) = v$, and therefore $h(u+x) = h(u) + h(x)$. We have proved that h is an automorphism of $Q(+)$. Thus f_1, g_1 are automorphisms of $Q(+)$ and it follows that Q is a medial quasigroup. Finally, H is generated by f_1, g_1 and G is finite by 3.6. □

Remark 4.3. All c-simple medial quasigroups are described in [2]. Especially, every such a quasigroup is finite and of prime power order.

References

[1] Itô N., *Über das Produkt von zwei abelschen Gruppen*, Math. Z. **62** (1955), 400–401.
[2] Ježek J., Kepka T., *Varieties of abelian quasigroups*, Czech. Math. J. **27** (1977), 473–503.
[3] Kepka T., *Multiplication groups of some quasigroups*, Colloq. Math. Soc. J. Bolyai **29** (1977), 459–465.
[4] ———, *Quasigroups having at most three inner mappings*, Acta Univ. Carolinae Math. Phys. **30** (1989), 3–11.

Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 00 Praha 8, Czech Republic

Catedra de algebra, Universitateu de Stat diu Rep. Moldova, Strada Mateevici 60, Chişinău 14, Moldova

(*Received* November 27, 1992)