Commentationes Mathematicae Universitatis Carolinae

Aleš Drápal; Tomáš Kepka

Parity of orthogonal automorphisms

Commentationes Mathematicae Universitatis Carolinae, Vol. 28 (1987), No. 2, 251--259

Persistent URL: http://dml.cz/dmlcz/106538

COMMENTATIONES MATHEMATICAE UNIVERSITATIS CAROLINAE
28,2(1987)

PARITY OF ORTHOGONAL AUTOMORPHISMS

Aleš DRÁPAL and Tomáš KEPKA

Abstract: The parity of orthogonal automorphisms of some finite abelian groups is investigated.

Key words: Parity, orthogonal, automorphism.

Classification: 20B25

The concept of orthogonal permutations of groups is well known and these permutations were used by many authors in various situations (see e.g. [1] for further details and references). In the present note, we are investigating the parity of orthogonal automorphisms of some finite abelian groups. The results allow us to construct idempotent quasigroups with prescribed order and parity of translations.

1. Introduction. Let Q be a quasigroup (i.e. a groupoid with the unique division). For each $a \in Q$, we have two transformations of the underlying set Q; they are called the left and the right translation by a and they are defined by $\mathcal{L}(a,Q)(x)=ax$ and $\mathcal{R}(a,Q)(x)=xa$ for every $x \in Q$. Since Q is a quasigroup, both these transformations are permutations, and hence they belong to the permutation group $\mathcal{S}(Q)$ of Q. We put $\mathcal{M}_l(Q)=\langle \mathcal{L}(a,Q); a \in Q \rangle \subseteq \mathcal{S}(Q)$; $\mathcal{M}_r(Q)=\langle \mathcal{R}(a,Q); a \in Q \rangle$ and $\mathcal{M}(Q)=\langle \mathcal{M}_l(Q) \cup \mathcal{M}_r(Q) \rangle$.

A quasigroup Q is said to be

- of type (1) if $\mathcal{M}(Q) \subseteq \mathcal{A}(Q)$ (the alternating group);
- of type (2) if $\mathcal{M}_l(Q) \subseteq \mathcal{A}(Q)$ and $\mathcal{R}(a,Q) \notin \mathcal{A}(Q)$ for each $a \in Q$;
- of type (3) if $\mathcal{M}_r(Q) \subseteq \mathcal{A}(Q)$ and $\mathcal{L}(a,Q) \notin \mathcal{A}(Q)$ for each $a \in Q$;
- of type (4) if $\mathcal{L}(a,Q), \mathcal{R}(a,Q) \notin \mathcal{A}(Q)$ for each $a \in Q$.

1.1. Lemma. Let $n \geq 2$, $S_1,\dots,S_n$ be finite sets of orders $m_1,\dots,m_n$, resp. and let $f_1 \in \mathcal{S}(S_1),\dots,f_n \in \mathcal{S}(S_n)$. Put $S=S_1 \times$

$\times \ldots \times S_n$, $f=f_1\times \ldots \times f_n$ and $n_i=m_1,\ldots,m_n/m_i$, $i=1,2,\ldots,n$. Then $\mathrm{sgn}(f)=\prod_{i=1}(\mathrm{sgn}(f_i))^{n_i}$. In particular, if $n=2$, then $\mathrm{sgn}(f)=$ $=\mathrm{sgn}(f_1)^{m_2}\cdot \mathrm{sgn}(f_2)^{m_1}$.

2. Orthogonal and complete mappings. In this section, let G be a group. A permutation h of G is said to be complete if the mapping $x \to h(x)x$ is again a permutation of G and, moreover, $h(1)=1$. An ordered pair (f,g) of permutations of G is said to be a pair of orthogonal permutations of G if $f(x^{-1})x=g(x)$ for every $x\in G$ and, moreover, $f(1)=1$. The permutation g (which is determined uniquely) is then called the orthogonal mate of f. A permutation of G is called orthogonal if it possesses the orthogonal mate.

Now, we shall formulate some easy observations concerning orthogonal and complete mappings. They are collected here just for the sake of reference.

2.1. Lemma. A pair (f,g) of permutations of G is a pair of orthogonal permutations iff the pair (g,f) is so.

2.2. Lemma. (i) If (f,g) is a pair of orthogonal permutations of G, then the mappings $x \to f(x)x^{-1}=g(x^{-1})$ and $x \to f(x^{-1})=$ $=g(x)x^{-1}$ are complete permutations.

(ii) If h is a complete permutation of G, then the mapping $x \to h(x^{-1})x^{-1}$ is a complete permutation and $(x \to h(x^{-1}), x \to h(x)x$ is a pair of orthogonal permutations of G.

2.3. Lemma. (i) If G is finite and f is an automorphism of G, then f is orthogonal iff $f(x)\neq x$ for any $1\neq x\in G$.

(ii) If G is finite and commutative and h is an automorphism of G, then h is complete iff $h(x)\neq x^{-1}$ for any $1\neq x\in G$.

2.4. Lemma. Let H be a group, (f,g) a pair of orthogonal permutations of G and (h,k) a pair of orthogonal permutations of H. Put $K=G\times H$, $p=f\ \ h$ and $q=g\times k$. Then (p,q) is a pair of orthogonal permutations of the group K. Moreover, if both f and h (resp. g and k) are automorphisms, then p (resp. q) is an automorphism.

2.5. Lemma. Let (f,g) be a pair of orthogonal permutations

of G. The following conditions are equivalent:
(i) Both f and g are automorphisms of G.
(ii) G is commutative and f is an automorphism.
(iii) G is commutative and g is an automorphism.

Now, suppose that G is finite. We denote by $Op_1(G)$ (resp. $Op_2(G)$, $Op_3(G)$, $Op_4(G)$) the set of pairs (f,g) of orthogonal permutations such that sgn(f)=1=sgn(g) (resp. sgn(f)=1, sgn(g)= =-1; sgn(f)=-1, sgn(g)=1; sgn(f)=-1=sgn(g)). Moreover, if G is commutative (see 2.5) and $1 \leq i \leq 4$, then we put $Oa_i(G)=Op_i(G) \cap \cap (Aut(G) \times Aut(G))$.

3. <u>Orthogonal mappings and idempotent quasigroups</u>. In this section, let G be a group and (f,g) a pair of orthogonal permutations of G. We shall define a new binary operation, say $\circ$, on G by $x \circ y=f(xy^{-1})y=g(yx^{-1})x$ for all $x,y \in G$ and we denote by $\mathcal{O}(G,f)$ the corresponding groupoid $G(\circ)$. It is easy to see that $G(\circ)$ is an idempotent quasigroup. The following results are clear.

3.1. <u>Lemma</u>. Put $G(*)=\mathcal{O}(G,g)$. Then the quasigroups $G(\circ)$ and $G(*)$ are opposite, i.e. $x \circ y=y * x$ for all $x,y \in G$.

3.2. <u>Lemma</u>. $\mathcal{R}(x,G(\circ))=\mathcal{R}(x,G)f\,\mathcal{R}(x^{-1},G)=\mathcal{R}(x,G)f\,\mathcal{R}(x,G)^{-1}$ and $\mathcal{L}(x,G(\circ)=\mathcal{R}(x,G)g\,\mathcal{R}(x^{-1},G)=\mathcal{R}(x,G)g\,\mathcal{R}(x,G)^{-1}$. In particular, $\mathcal{R}(1,G(\circ))=f$ and $\mathcal{L}(1,G(\circ))=g$.

3.3. <u>Lemma</u>. Suppose that f (resp. g) is an automorphism of G. Then $\mathcal{R}(x,G(\circ))=\mathcal{R}(g(x),G)f$ (resp. $\mathcal{L}(x,G(\circ))=\mathcal{R}(f(x),G)g$) and $\mathcal{M}_r(G(\circ))=\langle \mathcal{M}_r(G),f\rangle$ (resp. $\mathcal{M}_l(G(\circ))=\langle \mathcal{M}_r(G),g\rangle$).

3.4. <u>Lemma</u>. Suppose that f, g are automorphisms of G. Then $\mathcal{M}(G(\circ))=\langle \mathcal{M}_r(G),f,g\rangle$.

3.5. <u>Lemma</u>. (i) $hMh^{-1}=M$ for any $h \in \mathcal{M}_r(G)$, where $M=\{\mathcal{R}(x,G(\circ));x \in G\}$.

(ii) $hNh^{-1}=N$ for any $h \in \mathcal{M}_r(G)$, where $N=\{\mathcal{L}(x,G(\circ));x \in G\}$.

(iii) The group $\mathcal{M}_r(G)$ is contained in each of the groups $\mathcal{N}_{\mathcal{G}(G)}(\mathcal{M}_r(G(\circ)))$, $\mathcal{N}_{\mathcal{G}(G)}(\mathcal{M}_l(G(\circ)))$ and $\mathcal{N}_{\mathcal{G}(G)}(\mathcal{M}(G(\circ)))$.

3.6. <u>Lemma</u>. Suppose that G is finite.

(i) If both f and g are even, then $G(\circ)$ is of type (1).

(ii) If f is odd and g is even, then $G(\circ)$ is of type (2).

(iii) If f is even and g is odd, then $G(\circ)$ is of type (3).

(iv) If both f and g are odd, then $G(\circ)$ is of type (4).

3.7. Lemma. If f is an automorphism of G, then $x\circ y=$ $=f(x)g(y)$. If g is an automorphism of G, then $x\circ y=g(y)f(x$.

An idempotent quasigroup Q is said to be orthomorphic if there exist an abelian group $Q(+)$ with the same carrier and a pair (f,g) of orthogonal automorphisms such that $Q(\circ)=$ $=\mathcal{O}(Q(+),f)$. An idempotent quasigroup Q is said to be orthostrophic (left orthomorphic, right orthomorphic) if there exist a group $Q(+)$ (not necessarily commutative) and a pair (f,g) of orthogonal mappings such that $Q=\mathcal{O}(Q(+),f)$ (and f is an automorphism, g is an automorphism of $Q(+)$). Clearly, orthostrophic (left orthomorphic, right orthomorphic, orthomorphic) idempotent quasigroups are closed under cartesian products.

3.8. Remark. For a group G and a pair (f,g) of orthogonal permutations of G we could define an idempotent quasigroup $\overline{\mathcal{O}}(G,f)=G(\odot)$ by $x\odot y=xf(x^{-1}y)=yg(y^{-1}x)$. Then $\mathcal{L}(x,G(\odot))=$ $=\mathcal{L}(x,G)f\mathcal{L}(x,G)^{-1}$ and $\mathcal{R}(x,G(\odot))=\mathcal{L}(x,G)g\mathcal{L}(x,G)^{-1}$. If $\overline{G}$ is the group opposite to G, then $\overline{\mathcal{O}}(G,f)=\mathcal{O}(\overline{G},g)$.

4. Orthogonal automorphisms of cyclic groups. In this section, let $n\geq 3$ be an odd positive integer (cyclic groups of even orders and infinite cyclic groups have no orthogonal automorphisms) and let $G=G(+)=Z_n(+)=\{0,1,\dots,n-1\}$ (the additive group of integers modulo n). Further, denote by $G^*=Z_n^*$ the multiplicative group of invertible elements of the ring Z_n. Hence $G^*=\{i;1\leq i\leq$ $\leq n-1,\gcd(i,n)=1\}$ and $\mathrm{card}(G^*)=\varphi(n)$, where φ denotes the Euler function. Notice that $\varphi(n)$ is an even number. For any $m\in G^*$ we have an automorphism f_m of G defined by $f_m(x)=mx$ for each $x\in G$. Since G is a cyclic group, every automorphism f of G is equal to f_m for some $m\in G^*$ and the mapping $f\longrightarrow m$ is an isomorphism of Aut(G) onto G^*. For $m\in G^*$, let $s(m)=s_n(m)=\mathrm{sgn}(f_m)$.

4.1. Lemma. The following conditions are equivalent for $m\in G^*$:

(i) $f=f_m$ is orthogonal.

(ii) $m-1 \in G^*$.

In this case the mapping $g: x \longrightarrow (1-m)x=(m-1)(-x)=(nm-n-m+1)x$ is the orthogonal mate of f. Moreover, $sgn(g)=s(n-1)s(m-1)$.

4.2. Lemma. $n-1 \in G^*$ and $s(n-1)=(-1)^{(n-1)/2}$.

Proof. f_{n-1} is composed from $(n-1)/2$ 2-cycles.

4.3. Suppose that $n=p^r$, where $p \geq 3$ is a prime and $r \geq 1$. Let $2 \leq m \leq p^r-1$ be such that m generates the group G^*. We shall find the decomposition of f_m into cycles. If $r=1$ then f_m is a $(p-1)$-cycle (since m generates $Z_p^*=Z_p-\{0\}$), and hence $sgn(f_m)=s_p(m)= -1$. Assume that $r \geq 2$ and, for every $i=0,1,\dots,r-1$, let A_i be the set of $j \in G$ such that p^i divides j and p^{i+1} does not (in Z). Then $G-\{0\}$ is the disjoint union of the sets A_i and $f_m(A_i)=A_i$ for any i. Moreover, $card(A_i)=p^{r-i-1}(p-1)$ are even numbers. Clearly, the set A_i contains just all elements from G which have order p^{r-1} in G. However, each subgroup of G is cyclic, and hence, if $a,b \in A_i$, then $b=ja$ for some $j \in G^*$. But j is a power of m and now it is clear that $f_m|A_i$ is a cycle. In particular, $sgn(f_m)=(-1)^r$.

4.4. Lemma. Suppose that $n=p^r$, where $p \geq 3$ is a prime and $r \geq 1$. Let $m \in G^*$ be a generator of G^*.

(i) $s(m)=(-1)^r$.

(ii) If r is even, then every automorphism of G is even and $s(i)=1$ for every $i \in G^*$.

(iii) If r is odd, then card $\{i \in G^*; s(i)=1\}$ =card $\{i \in G^*; s(i)=-1\}=p^{r-1}(p-1)/2$.

Proof. See 4.3.

4.5. Lemma. Let $n=p^r$, where $p \geq 3$ is a prime and either $p \geq 7$, or $p \in \{3,5\}$ and r is even. Then there exists $i \in G^*$ such that $i+1 \in G^*$ and $s(i)=s(i+1)=1$.

Proof. If either $n=7$ or $p \in \{3,5\}$, then we can put $i=1$ (use 4.4(ii)). Now, assume that $p \geq 7$, $n \geq 11$ and that the assertion is not true. Then $s(1)=1$, $s(2)=-1$, $s(4)=s(2)s(2)=1$, $s(5)=-1$, $s(9)=$ $=s(3)s(3)=1$, $s(10)=s(2)s(5)=1$, a contradiction.

4.6. Lemma. Let $n=p^r$, where $p \geq 3$ is a prime and $r \geq 2$. Then $s(kp+1)=1$ for every $0 \leq k \leq p^{r-1}-1$.

Proof. $(kp+1)^{p^{r-1}}=1$ in G (by induction on r), f_{kp+1} is an automorphism of odd order and $s(kp+1)=1$.

4.7. <u>Lemma</u>. Let $n=p^r$, where $p\geq 3$ is a prime and r is odd. Then there exists $i\in G^*$ such that $i+1\in G^*$ and $s(i)=1$, $s(i+1)=-1$.

Proof. Let $m\in G^*$ be a generator of this group. There exist $0\leq k\leq p^{t-1}-1$ and $1\leq j\leq p-1$ such that $m=kp+j$. Consider the numbers $kp+1, kp+2,\dots,kp+p-1$. By 4.6 and 4.4(i), $s(kp+1)=1$ and $s(kp+j)=$ $=-1$. The assertion is now clear.

4.8. <u>Lemma</u>. Let $n=p^r$, where $p\geq 3$ is a prime and r is odd. Then $\mathrm{card}\{i;1\leq i\leq p-1,s(i)=1\}=\mathrm{card}\{i;1\leq i\leq p-1,s(i)=-1\}=$ $=(p-1)/2$.

Proof. There are p^{r-1} elements in G^* of the form $kp+1$. As $(kp+1)^{p^{r-1}}=1$ in G, the Sylow p-subgroup $S<G^*$ is formed exactly by all these elements. Consider the set $P=\{1,2,\dots,p-1\}$. If $i=f_{kp+1}(j)$ for any $i,j\in P$, then $i-j$ is divisible by p, and hence $i=j$. Therefore $G^*=PS=SP$, and by 4.6 $\mathrm{card}\{i\in G^*;s(i)=1\}=$ $=\mathrm{card}(S)\cdot\mathrm{card}\{i\in P;s(i)=1\}$. The rest follows from 4.4(iii).

4.9. <u>Lemma</u>. Let $n=p^r$, where $p\geq 5$ is a prime and r is odd. Then there exists $i\in G^*$ such that $i+1\in G^*$ and $s(i)=s(i+1)=-1$.

Proof. Assume that this is not true.. As $s(1)=1$, by 4.8 we have $s(2i-1)=1$, $s(2i)=-1$ for any $1\leq i\leq (p-1)/2$. However, $s(4)=$ $=s(2)s(2)=1$.

4.10. <u>Lemma</u>. Let $n=p^r$, where $p\geq 5$ is a prime and r is odd. Then there exists $i\in G^*$ such that $i+1\in G^*$ and $s(i)=-1$, $s(i+1)=1$.

Proof. Assume that this is not true. We have $s(1)=1$, $s(4)=$ $=s(2)s(2)=1$, and hence $s(2)=s(3)=1$. Now, by induction on i, we are going to show that $s(i)=1$ for any $i\in G^*$, $p>i>4$. If i is not a prime, then $s(q)=1$ for each prime divisor q of i, and so $s(i)=$ $=1$. If i is a prime, then $p>i+1$, $i+1$ is even, $s(i+1)=1$, and so $s(i)=1$.

4.11. <u>Lemma</u>. Let $p=2k+1$, $k\geq 1$, be a prime.

(i) If k is even, then 4 divides p^r-1 for any $r\geq 1$.

(ii) If k is odd, then 4 divides p^r-1 iff r is even.

Proof. We have $p^{r+1}-1=p(p^r-1)+p-1$.
Put $\mathrm{specc}(n)=\{i; 1\leq i\leq 4, Ca_i(G)\neq\emptyset\}$.

4.12. Proposition. Let $n=p_1^{r_1}\dots p_u^{r_u}$, where $1\leq u, r_1,\dots,r_u$ and $3\leq p_1<p_2<\dots<p_u$ are odd primes.
(i) If $p_i\geq 7$ and r_i are odd for some $1\leq i\leq u$, then $\mathrm{specc}(n)=\{1,2,3,4\}$.

(ii) If $p_1=3$, r_1 is odd and the numbers $r_2,\dots,r_u$ are even, then $\mathrm{specc}(n)=\{4\}$.

(iii) If all the numbers r_i are even, then $\mathrm{specc}(n)=\{1\}$.

(iv) If either $p_1=3$, $p_2=5$, r_2 is odd and the numbers $r_1, r_3,\dots,r_u$ are even or $p_1=5$, r_1 is odd and the numbers $r_2,\dots,r_u$ are even, then $\mathrm{specc}(n)=\{2,3,4\}$.

(v) If $p_1=3$, $p_2=5$, r_1, r_2 are odd and $r_3,\dots,r_u$ are even, then $\mathrm{specc}(n)=\{1,2,3\}$.

Proof. The ring Z_n is isomorphic to the cartesian product of the rings Z_{n_i}, $n_i=p_i^{r_i}$. The assertion may be now derived easily from 1.1, 2.4 and the results of this section.

5. Orthogonal automorphisms and finite fields. In this section, let T be a finite field of order $n=p^r$, $p\geq 2$ a prime and $r\geq 1$. For every $a\in T^*=T-\{0\}$ we have an automorphism f_a of $T(+)=T$ defined by $f_a(x)=ax$. We put $s(a)=s_T(a)=\mathrm{sgn}(f_a)$.

The prime subfield of T will be denoted by P.

5.1. Lemma. (i) If $p=2$ then $s(a)=1$ for every $a\in T^*$.

(ii) If $p\geq 3$, then $\mathrm{card}\,\{a\in T^*; s(a)=1\}=\mathrm{card}\,\{a\in T^*; s(a)=-1\}=(n-1)/2$.

Proof. (i) T^* is a group of odd order.

(ii) If $a\in T^*$ is a generator of T^*, then $s(a)=-1$. The rest is clear.

5.2. Lemma. Suppose that $p\geq 3$ and $r\geq 2$. Then there exist $a,b,d\in T-P$ such that $s(a)=s(a^{-1})=s(a^{-1}+1)=s(d+1)=-1$ and $s(d)=s(a+1)=s(b)=s(b+1)=1$.

Proof. If $c\in T-P$, $s(c)=-1$, then $s(c^{-1})=-1$ and $s(c+1)=$

$=s(c)s(c^{-1}+1)=-s(c^{-1}+1)$. If $s(c^{-1}+1)=-1$, we put $a=c$, otherwise $a=c^{-1}$. Further, put $d=a+\max\{i; s(a+i)=1 \text{ and } 1\leq i<p\}$. If $s(a+2)=1$, we put $b=a+1$; in the other case let $b=a(a+2)$. Then $s(b)=s(a)s(a+2)=1$ and $s(b+1)=s(a+1)s(a+1)=1$.

Put $\mathrm{specf}(n)=\{i; 1\leq i\leq 4,\ Oa_i(T(+))\cap(L\times L)\neq\emptyset\}$, where $L=\{f_a a\in T^*\}$.

5.3. Proposition. Let $n=p^r$, $p\geq 2$ a prime and $r\geq 1$.
(i) If $p\geq 7$, then $\mathrm{specf}(n)=\{1,2,3,4\}$.

(ii) If $p=2$ and $r\geq 2$, then $\mathrm{specf}(n)=\{1\}$.

(iii) If $p\geq 3$ and $r\geq 2$, then $\mathrm{specf}(n)=\{1,2,3,4\}$.

(iv) $\mathrm{specf}(2)=\emptyset$, $\mathrm{specf}(3)=\{4\}$ and $\mathrm{specf}(5)=\{2,3,4\}$.

Proof. Use 5.1, 5.2 and 4.12.

6. Summary. For a positive integer n, let $\mathrm{spec}(n)$ designate the set of $1\leq i\leq 4$ such that $Oa_i(G)$ is non-empty for a finite abelian group of order n.

6.1. Proposition. Let $n\geq 3$ be odd.
(i) If n is divisible by a prime ≥ 7, then $\mathrm{spec}(n)=\{1,2,3,4\}$.

(ii) If n is divisible either by 9 or by 25, then $\mathrm{spec}(n)=\{1,2,3,4\}$.

(iii) $\mathrm{spec}(3)=\{4\}$, $\mathrm{spec}(5)=\{2,3,4\}$ and $\mathrm{spec}(15)=\{1,2,3\}$.

Proof. Apply 4.12, 5.3, 2.4 and 1.1.

6.2. Proposition. Let $n\geq 4$ be an even number divisible by 4. Then $1\in\mathrm{spec}(n)$.

Proof. Apply 6.1, 5.3, 2.4 and 1.1.

6.3. Corollary. $1\in\mathrm{spec}(n)$, provided either $n\geq 7$ is odd or n is even and divisible by 4.

6.4. Corollary. $4\in\mathrm{spec}(n)$, provided n is odd and $n\neq 15$.

6.5. Corollary. $3,2\in\mathrm{spec}(n)$, provided $n\geq 5$ is odd.

6.6. Corollary. Let $n\geq 2$ be an integer.

(i) If either $n \geq 7$ is odd or n is divisible by 4, then there exists an orthomorphic idempotent quasigroup of type (1) and order n.

(ii) If $n \geq 5$ is odd, then there exists an orthomorphic idempotent quasigroup of type (2) (resp. (3)) and order n.

(iii) If $n \neq 15$ is odd, then there exists an orthomorphic idempotent quasigroup of type (4) and order n.

Reference

[1] J. DÉNES, A.D. KEEDWELL: Latin squares and their applications, Akadémiai Kiadó, Budapest, 1974.

(Oblatum 12.2. 1987)

Matematicko-fyzikální fakulta, Sokolovská 83, 18600 Praha 8, Czechoslovakia