Alternating Groups and Latin Squares

ALEŠ DRÁPAL AND TOMÁŠ KEPKA

For every \( n \geq 1 \), \( n \neq 2, 4, 5 \), the alternating group \( A(n) \) on \( n \) symbols is equal to the multiplication group of a loop.

1. Introduction

The aim of this short note is to show that, for \( n \geq 2, 4, 5 \), the alternating group in its natural action on \( n \) letters is similar to the action of the multiplication group or left multiplication group of a loop on the \( n \) letters. In particular, the alternating group is a Latin square group in the sense of [1].

For a non-empty finite set \( M \), let \( \mathcal{S}(M) \) denote the symmetric group and \( A(M) \) the alternating group on \( M \). If \( G \) is a subgroup of \( \mathcal{S}(M) \), then \( \mathcal{N}(G) \) will be the normalizer of \( G \) in \( \mathcal{S}(M) \).

In the sequel, we shall make use of the following well known results:

(1.1) Proposition. Let \( G \leq \mathcal{S}(M) \) be a subgroup primitive on \( M \). Then \( A(M) \leq G \), provided that at least one of the following five conditions is satisfied:

(i) \( G \) contains a \( q \)-cycle for some \( q \geq 2 \) such that \( 2q + 1 \leq \text{card}(M) \);
(ii) \( G \) contains a \( p \)-cycle for a prime \( p \geq 2 \) such that \( p + 3 \leq \text{card}(M) \);
(iii) \( G \) contains a 3-cycle;
(iv) \( \text{card}(M) \geq 9 \) and \( G \) contains the composition of two different transpositions;
(v) \( G \) is 2-transitive and contains a permutation of degree less than \( (n - 2\sqrt{n})/3 \).

Proof. (i) See [6, Theorem 13.5].
(ii) See [6, Theorem 13.9].
(iii) See [6, Theorem 13.3].
(v) See [6, Theorem 15.1].
(iv) With respect to (iii), we can assume that the set \( P \) of permutations \( f \in G \) of type \( (2, 0, 0, \ldots) \) is non-empty and we denote by \( H \) the subgroup generated by \( P \). Since \( H \) is normal in \( G \) and \( G \) is primitive on \( M \), \( H \) is transitive on \( M \). For each \( f \in P \), put \( A(f) = \{ x \in M; f(x) \neq x \} \). Then \( \text{card}(A(f)) = 4 \) and the rest of the proof is divided into several parts: (a) Let \( A = A(f) = A(g) \) for some \( f, g \in P, f \neq g \). Then the subgroup \( K = \{ h \in H; h(M - A) = \text{id} \} \) is transitive on \( A \) and the result follows from [6, Theorem 13.5].
(b) Let \( \text{card}(A(f) \cup A(g)) \in \{ 5, 7 \} \) for some \( f, g \in P \). Then \( (fg)^2 \) is either a 3-cycle or a 5-cycle and we can use (ii).
(c) Let \( f, g \in P, f = (x y)(u v), g = (x u)(z w), N = \{ x, y, u, v, z, w \} \leq M, \text{card}(N) = 6 \). Then \( gfg = (x v)(y u) \) and (a) may be applied.
(d) Suppose that neither (a) nor (b) nor (c) can be applied. Then \( \text{card}(A(f) \cup A(g)) \in \{ 6, 8 \} \) for all \( f, g \in P, f \neq g \) and, moreover, since \( H \) is transitive on \( M \), there exist \( f, g \in P \) such that \( f = (x y)(u v) \) and \( g = (x z)(u w) \) for some \( N = \{ x, y, u, v, z, w \} \leq M, \text{card}(N) = 6 \). Put \( U = \{ x, y, z \} \) and \( V = \{ u, v, w \} \). Then these sets satisfy the following condition:

There exists a bijection \( F: U \rightarrow V \) such that for every \( k \in \mathcal{S}(U) \) there is a permutation \( p \in G \) with \( p|U = k, p|V = FkF^{-1} \) and \( p|(M - (U \cup V)) = \text{id} \).
Now, suppose that $U, V$ are two disjoint subsets of $M$ satisfying this condition and such that $\text{card}(U)$ is maximal. Since $H$ is transitive on $M$, there exists $q = (a\ b)(c\ d) \in P$ such that $a \in U$ and $b \notin U$. Now, we have to distinguish the following cases:

1. $c \in U$ or $d \in U$. Suppose $c \in U$, the other case being similar. Then $p = (a\ c)(F(a)\ F(c)) \in G$ and the result follows by one of (a), (b) or (c).
2. $c \notin V$ and $d \notin V$. With respect to (1), we can assume that $c, d \notin U$. Take $e \in U$ such that $a \neq e$. Then $p = (a\ e)(F(a)\ F(e))$ is in $G$ and the result follows by (b) or (c).
3. $c, d \in V$. Then $p = (c\ d)(F^{-1}(c)\ F^{-1}(d)) \in G$. If $a \neq F^{-1}(c), F^{-1}(d)$, then we can use (1) (where $q$ is replaced by $pq$). In the opposite case, $pq$ is a 3-cycle.
4. $c \in V, d \in M - (U \cup V)$ and $b \in V$. Then $p = (b\ c)(F^{-1}(b)\ F^{-1}(c))$ is in $G$ and the result follows by (b) or (c).
5. $c = F(a)$ and $b, d \in M - (U \cup V)$ Put $U' = U \cup \{b\}, V' = V \cup \{d\}$ and extend $F$ to $F'$ by $F'(b) = d$. Then we obtain a contradiction with the maximality of $\text{card}(U)$.

Further, we shall need the following simple assertion:

\textbf{(1.2) Lemma.} Let $f \in \mathcal{F}(M), g \in \mathcal{F}(N)$ and $m = \text{card}(M), n = \text{card}(N)$. Then $\text{sgn}(f \times g) = \text{sgn}(f)^m \times \text{sgn}(g)^n, f \times g \in \mathcal{F}(M \times N)$.

A quasi-group $Q$ is a groupoid with unique division, i.e. the left and right translations $\mathcal{L}(a, Q)$ and $\mathcal{R}(a, Q)$ of $Q$ ($\mathcal{L}(a, Q)(x) = ax$ and $\mathcal{R}(a, Q)(x) = xa$ for all $x \in Q$) are permutations of $Q$ for every $a \in Q$. The subgroup $\mathcal{M}(Q)$ (resp. $\mathcal{M}_0(Q)$) of $\mathcal{F}(Q)$ generated by all left (resp. right) translations is called the left (resp. right) multiplication group of $Q$. The subgroup $\mathcal{M}_0(Q)$ generated by $M(Q) \cup \mathcal{M}_0(Q)$ is called the multiplication group of $Q$.

Throughout this paper, $Z = Z(\pm)$ will denote the additive group of integers and, for $n \geq 1$, $Z_n(\pm) = \{0, 1, 2, \ldots, n - 1\}$ the additive group of integers modulo $n$.

2. Orthostrophic Idempotent Quasigroups and Their Prolongations

Let $Q$ be a finite idempotent quasigroup and $e \notin Q$. We denote by $P = P(\ast) = \mathcal{P}(Q, e)$ the corresponding prolongation of $Q$. That is, $P = Q \cup \{e\}, x \ast y = xy, x \ast x = e \ast e = e$ and $x \ast e = x = e \ast x$ for all $x, y \in Q, x \neq y$. Then $P$ is a loop (i.e. a quasigroup with identity element). For $f \in \mathcal{F}(Q)$, we define $f \in \mathcal{F}(P)$ by $f|Q = f$ and $f(e) = e$. Now, we have the following two obvious results:

\textbf{(2.1) Lemma.} $\text{sgn}(\mathcal{L}(x, Q)) = -\text{sgn}(\mathcal{L}(x, P))$ and $\text{sgn}(\mathcal{R}(x, Q)) = -\text{sgn}(\mathcal{R}(x, P))$ for all $x \in Q$.

\textbf{(2.2) Lemma.} Let $M = \{\mathcal{L}(x, Q); x \in Q\}$ (resp. $M = \{\mathcal{R}(x, Q); x \in Q\}$) and $N = \{\mathcal{L}(x, P); x \in P\}$ (resp. $N = \{\mathcal{R}(x, P); x \in P\}$). If $fM = Mf$ for some $f \in \mathcal{F}(Q)$, then $fN = Nf$.

Let $G$ be a finite group and $f, g \in \mathcal{F}(G)$. Then $(f, g)$ is said to be a pair of orthogonal permutations of $G$ if $f(1) = 1$ and $g(x) = f(x^{-1})x$ for each $x \in G$. In this case, we can define an idempotent quasigroup $G(\circ) = \mathcal{O}(G, f)$ by $x \circ y = f(xy^{-1})y$ for all $x, y \in G$ (this construction as well as the concept of orthogonal permutations have been studied by various authors; see [2] for further details and references). Every idempotent quasigroup constructed in this way will be called orthostrophic (left orthomorphic if $f$ is an automorphism of $G$, right orthomorphic if $g$ is an automorphism and orthomorphic if both $f$ and $g$ are automorphisms; in the last case $G$ is necessarily commutative). The following assertions are clear:
(2.3) **Lemma.** (i) $L(x, G(\sigma)) = R(x, G)gR(x, G)^{-1}$ and $R(x, G(\sigma)) = R(x, G)fR(x, G)^{-1}$ for each $x \in G$.
(ii) $\text{sgn}(L(x, G(\sigma))) = \text{sgn}(g)$ and $\text{sgn}(R(x, G(\sigma))) = \text{sgn}(f)$ for each $x \in G$.
(iii) $R(x, G(y))M = M R(x, G(y))$ and $R(x, G(y))N = N R(x, G(y))$ for each $x \in G$, where $M = \{L(x, G(\sigma)); x \in G\}$ and $N = \{R(x, G(\sigma)); x \in G\}$.

Now, let $e \notin G$ and $P = P(\star) = \mathcal{P}(G(\sigma), e)$.

(2.4) **Lemma.** $kM(P) = M(P)k$, $kM_i(P) = M_i(P)k$ and $kM_\sigma(P) = M_\sigma(P)k$ for all $k = R(x, G)$, $x \in G$.

(2.5) **Lemma.** The permutation groups $\mathcal{N}(M_i(P))$, $\mathcal{N}(M_\sigma(P))$ and $\mathcal{N}(M_\alpha(P))$ are 2-transitive on $P$.

**Proof.** By (2.2) and (2.3, iii), $R(x, G) \in \mathcal{N}(M_i(P))$ for every $x \in G$. Consequently, the stabilizer of $e$ in $\mathcal{N}(M_i(P))$ is transitive on $G = P - \{e\}$. Since $M_i(P)$ is transitive on $P$, $\mathcal{N}(M_\sigma(P))$ is so, and hence it is 2-transitive; and similarly for the other cases.

(2.6) **Lemma.** Suppose that $G$ is non-trivial and $f$ is an automorphism of $G$ (i.e. $G(\sigma)$ is left orthomorphic). Then the permutation groups $\mathcal{N}(M_i(P))$ and $\mathcal{N}(M_\sigma(P))$ contain 3-cycles.

**Proof.** Let $1 \neq u \in G$ and $h = \overline{R(u^{-1}f(u), G)} \cdot R(u, P) \cdot R(1, P)^{-1}$. Then $h(e) = 1$, $h(1) = f(u)$, $h(f(u)) = e$ and $h(x) = x$ for every $x \in G$, $x \neq 1, f(u)$. Clearly, $h$ is contained in both the groups $\mathcal{N}(M_i(P))$ and $\mathcal{N}(M_\sigma(P))$.

(2.7) **Lemma.** Suppose that $G$ contains at least four elements and $f$ is an automorphism of $G$. Then $\mathcal{A}(P) \subseteq M_i(P)$.

**Proof.** By (2.5), (2.6) and (1.1, iii), $\mathcal{A}(P)$ is contained in $\mathcal{N}(M_i(P))$. Hence either $\mathcal{N}(M_\sigma(P)) = \mathcal{A}(P)$ or $\mathcal{N}(M_\sigma(P)) = \mathcal{P}(P)$. But $\mathcal{A}(P)$ is simple and the only non-trivial normal subgroup of $\mathcal{P}(P)$. Consequently, $\mathcal{A}(P) \subseteq M_i(P)$.

(2.8) **Proposition.** Let $n \geq 3$ be odd and $n \neq 15$. Then there exists an orthomorphic idempotent quasigroup $Q$ of order $n$ such that all translations of $Q$ are odd.

**Proof.** See [3, Corollary 6.4].

(2.9) **Proposition.** Let $k \geq 3$, $m \geq 1$, $m$ odd. Then there exists an orthostrophic idempotent quasigroup $Q$ of order $2^km$ such that all translations of $Q$ are odd and $\mathcal{R}(a, Q)^k$ is a 5-cycle for each element $a \in Q$. Moreover, if $m = 1$, then $L(b, Q)^k$ is a $k + 1$ cycle for some $b \in Q$.

**Proof.** See [4, Proposition 10.2, Lemma 10.3.5].

(2.10) **Example.** Let $G = Z_{15}$. Consider the following two 14-cycles $f, g \in \mathcal{L}(G)$:

$$f = (1 \ 13 \ 3 \ 11 \ 5 \ 9 \ 7 \ 8 \ 10 \ 6 \ 12 \ 4 \ 14 \ 2),$$
$$g = (1 \ 3 \ 7 \ 2 \ 5 \ 11 \ 10 \ 4 \ 9 \ 6 \ 13 \ 14 \ 12 \ 8).$$

Then $\text{sgn}(f) = \text{sgn}(g) = -1$ and $(f, g)$ is a pair of orthogonal permutations of $G$. Let $G(\sigma) = \mathcal{O}(G, f), e \notin G$ and $P = \mathcal{P}(G(\sigma), e)$. Then $P$ is a loop of order 16 and all translations of $P$ are even (see (2.1) and (2.3, ii)). Further, $h^6$ is a 7-cycle and $r = (t(q-1)^k)^2l(kq)^2$ is a...
3-cycle, where $h = \mathcal{R}(3, G)\mathcal{L}(0, P)$, $q = \mathcal{R}(0, P)$, $k = \mathcal{R}(2, G)$, $l = \mathcal{R}(14, G)$ and $t = \mathcal{R}(1, G)$. But $h^6 \in \mathcal{N}(\mathcal{M}_q(P))$ and $r \in \mathcal{N}(\mathcal{M}_q(P))$ by (2.2) and (2.3, iii), and consequently $\mathcal{M}_q(P) = \mathcal{M}_q(P) = \mathcal{A}(P)$ (see the proof of (2.7)).

(2.11) **PROPOSITION.** Let $n \geq 6$ be even. Then there exists a loop $L$ of order $n$ such that $\mathcal{M}(L) = \mathcal{M}(L) = \mathcal{A}(L)$.

**PROOF.** For $n \neq 16$, the result follows from (2.8), (2.1) and (2.7) (and its dual). For $n = 16$, see (2.10).

(2.12) **PROPOSITION.** Let $n \geq 9$ be such that $n - 1$ is divisible by 8. Then there exists a loop $L$ of order $n$ such that $\mathcal{M}(L) = \mathcal{M}(L) = \mathcal{A}(L)$.

**PROOF.** Consider the orthostrophic idempotent quasigroup $Q$ of order $n = 2$ by (2.9), and put $L = \mathcal{L}(Q, e)$, $e \notin Q$. Then $\mathcal{M}(L) \leq \mathcal{A}(L)$ by (2.1) and $\mathcal{M}(L)$ contains a 5-cycle. Now, by (2.5), (1.1, ii) and (2.1), $\mathcal{M}(L) = \mathcal{M}(L) = \mathcal{A}(L)$.

(2.13) **PROPOSITION.** Let $k \geq 3$ and $n = 2^k + 1$. Then there exists a loop $L$ of order $n$ such that $\mathcal{M}(L) = \mathcal{M}(L) = \mathcal{A}(L)$.

**PROOF.** Again, consider the orthostrophic quasigroup $Q$ of order $2^k$ by (2.9), and put $L = \mathcal{L}(Q, e)$, $e \notin Q$. Then $\mathcal{M}(L) = \mathcal{M}(L) = \mathcal{A}(L)$ (see the proof of (2.12)). Further, if $k$ is even, then $\mathcal{L}(b, P)^k$ is a $k + 1$-cycle for some $b \in P$ and we have $\mathcal{M}(L) = \mathcal{A}(L)$ by (1.1, i). Hence, assume that $k$ is odd. Then $\mathcal{L}(b, P)^k$ is a permutation of degree $k + 1$ from $\mathcal{N}(\mathcal{M}_q(P))$ and this permutation group is 2-transitive. Clearly, for $k \geq 5$, we have $k + 1 < (n - 2)/3$, and therefore $\mathcal{M}_q(P) = \mathcal{A}(P)$ by (1.1, v). For $k = 3$, the result follows from (1.1, v).

3. **ANOTHER TYPE OF PROLONGATION**

Let $n \geq 2$ be an integer and $Q$ a finite idempotent quasigroup of order $m \geq 1$. Further, let $R = Q \times Z_n$, $e \notin R \cup Z_n$, $S = Z_n \cup \{e\}$ and $P = R \cup \{e\}$.

First, we shall define an operation $\circ$ on $S$ as follows:

(i) $i \circ e = e \circ i = i$ for each $i \in Z_n$;
(ii) $i \circ j = i \oplus j \ominus 1$ for all $i, j \in Z_n$, $i + j \leq n - 2$ (in $Z$);
(iii) $i \circ j = i \oplus j$ for all $i, j \in Z_n$, $i + j \geq n$;
(iv) $i \circ e = e$ for all $i, j \in Z_n$, $i + j = n - 1$;
(v) $e \circ e = e$.

It is easy to check that $S(\circ)$ is a cyclic group of order $n + 1$. Now, we shall define an operation $\ast$ on $P$:

1. $x \ast e = e \ast x = x$ for each $x \in P$;
2. $(a, i) \ast (b, j) = (ab, i \oplus j)$ for all $a, b \in Q$, $a \neq b$, $i, j \in Z_n$;
3. $(a, i) \ast (a, j) = (a, i \circ j)$ for all $a \in Q$, $i, j \in Z_n$, $i \circ j \neq e$;
4. $(a, i) \ast (a, j) = e$ for all $a \in Q$, $i, j \in Z_n$, $i \circ j = e$.

Clearly, $P = P(\ast) = \mathcal{B}(Q, n, e)$ is a loop and it is commutative, provided that $Q$ is also.

(3.1) **LEMMA.** Let $a \in Q$, $i \in Z_n$ and $x = (a, i) \in R$.

(i) If $n$ is odd, then $\text{sgn}(\mathcal{L}(x, R)) = \text{sgn}(\mathcal{L}(a, Q))$ and $\text{sgn}(\mathcal{A}(x, R)) = \text{sgn}(\mathcal{A}(a, Q))$.
(ii) If both $n$ and $i$ are even, then $\text{sgn}(\mathcal{L}(x, R)) = \text{sgn}(\mathcal{A}(x, R)) = 1$.
(iii) If $n$ is even and $i$ odd, then $\text{sgn}(\mathcal{L}(x, R)) = \text{sgn}(\mathcal{A}(x, R)) = (-1)^n$. 

PROOF. Obviously, sgn($\mathcal{L}(i, Z_n)$) = 1 for $n$ odd and $(-1)^i$ for $n$ even. The rest follows by (1.2).

(3.2) LEMMA. Let $a \in Q$, $i \in Z_n$ and $x = (a, i) \in P$.

(i) If both $n$ and $i$ are odd, then sgn($\mathcal{L}(x, P)$) = sgn($\mathcal{L}(a, Q)$) and sgn($\mathcal{A}(x, P)$) = sgn($\mathcal{A}(a, Q)$).

(ii) If $n$ is odd and $i$ even, then sgn($\mathcal{L}(x, P)$) = $-\text{sgn}(\mathcal{L}(a, Q))$ and sgn($\mathcal{A}(x, P)$) = $-\text{sgn}(\mathcal{A}(a, Q))$.

(iii) If $n$ is even and $i$ odd, then sgn($\mathcal{L}(x, P)$) = \text{sgn}(\mathcal{A}(x, P)) = $(-1)^{m+1}$.

(iv) If both $n$ and $i$ are even, then sgn($\mathcal{L}(x, P)$) = sgn($\mathcal{A}(x, P)$) = 1.

PROOF. We have $\mathcal{L}(x, P) = \mathcal{L}(x, R)g_x$, where $g_x = \mathcal{L}(x, R)^{-1} \cdot \mathcal{L}(x, P)$ (here, for $f \in \mathcal{L}(R)$, $f \in \mathcal{L}(P)$ is defined by $f|_R = f$ and $f(e) = e$). However, sgn($\mathcal{L}(x, R)$) = sgn($\mathcal{L}(x, R)$) and $g_x(b, f) = (b, f)$ for all $a \neq b \in Q$ and $j \in Z_n$. Therefore, $\text{sgn}(g_x) = \text{sgn}(\mathcal{L}(i, Z_n)^{-1} \cdot \text{sgn}(h)$, $h = \mathcal{L}(i, S(r))$. Since $S(r)$ is a cyclic group of order $n+1$, we have $\text{sgn}(g_x) = (-1)^{i+1}$ for $n$ odd and $\text{sgn}(g_x) = (-1)^i$ for $n$ even. The result now follows from (3.1).

(3.3) LEMMA. If $n$ is even and $m$ odd, then $\mathcal{M}(P) \subseteq \mathcal{A}(P)$.

PROOF. See (3.2, iii, iv).

(3.4) LEMMA. Let $a \in Q$ and $f_a = \mathcal{L}((a, 1), P)^{-1} \cdot \mathcal{L}((a, 0), P)$. Then $f_a$ is composed from $m - 1$ $n$-cycles and one $n + 1$-cycle.

PROOF. $f_a$ is composed from $m - 1$ $n$-cycles of the form $((b, 0)(b, n-1)(b, n-2) \ldots (b, 1))$, $b \neq a$, and from the $n + 1$-cycle $(e(a, n-1)(a, n-2) \ldots (a, 1)(a, 0))$.

(3.5) LEMMA. Let $a \in Q$ and $h_a = \mathcal{L}(a, 1), P)^{-1} \cdot \mathcal{L}((a, 0), P)^2$. Then $h_a(e) = e$ and $h_a(b, 1) = (ab, 0)$ for each $b \in Q$, $b \neq a$.

PROOF. Easy.

(3.6) LEMMA. Let $m \geq 2$. Then the permutation groups $\mathcal{M}_r(P)$ and $\mathcal{M}_e(P)$ are 2-transitive.

PROOF. Let $a, b \in Q$, $a \neq b$ and $i \in Z_n$. Then $k(e) = e$ and $k(a, 0) = (a, i)$, where $k = f_b^{(n+1)/2}$ (where $k = f_b^{(n+1)/2}$). Further, $b = ca$ for some $c \in Q$, $c \neq a, b$, and we have $h_i(e) = e$ and $h_i(a, 1) = (b, 0)$. Now, it is easy to see that $\mathcal{M}_r(P)$ is 2-transitive. A similar proof applies for $\mathcal{M}_e(P)$.

(3.7) LEMMA. Let $m \geq 2$. Then $\mathcal{A}(P) \subseteq \mathcal{M}_r(P) \cap \mathcal{M}_e(P)$.

PROOF. By (3.6), $\mathcal{M}_r(P)$ is primitive, and by (3.4) it contains an $n + 1$-cycle. According to (1.1, i), $\mathcal{A}(P) \subseteq \mathcal{M}_r(P)$. Similarly, $\mathcal{A}(P) \subseteq \mathcal{M}_e(P)$.

(3.8) PROPOSITION. Let $k \geq 1$ and let $m \geq 3$ be odd. Then there exists a commutative loop $L$ of order $2^k m + 1$ such that $\mathcal{M}(L) = \mathcal{A}(L)$.

PROOF. Since $m$ is odd, we can define a multiplication on $Z_m$ by $ab = (a \oplus b)/2$. In this way, we obtain a commutative idempotent quasigroup $Q$ of order $m$. Now, the loop $L = P$ for $n = 2^k$ is commutative and $\mathcal{M}(L) = \mathcal{A}(L)$ by (3.3) and (3.7).
4. Summary

(4.1) Theorem. (i) For every $n \geq 1$, $n \neq 2, 4, 5$, there exists a loop $L$ of order $n$ such that $\mathcal{M}_1(L) = \mathcal{M}_r(L)) = \mathcal{M}(L) = \mathcal{A}(L)$.
(ii) If $L$ is a loop of order $\in \{2, 4, 5\}$, then none of the permutation groups $\mathcal{M}_1(L)$, $\mathcal{M}_r(L)$, $\mathcal{M}(L)$ is equal to $\mathcal{A}(L)$.

Proof. (i) For $n \geq 6$, see (2.11), (2.13) and (3.8). For $n = 1, 3$ we can put $L = Z_n$.
(ii) It is easy to check that every at most 4-element loop is an abelian group. Further, the complete list of 5-element loops (see, e.g., [2]) shows that every such non-associative loop has at least one odd left translation as well as at least one odd right translation.

(4.2) Remark. All symmetric and alternating groups (and hence also $\mathcal{A}(2)$, $\mathcal{A}(4)$ and $\mathcal{A}(5)$) are isomorphic to the multiplication group of a quasigroup (see [5]). On the other hand, one can show that the permutation groups $\mathcal{I}(3)$, $\mathcal{I}(4)$, $\mathcal{A}(4)$ and $\mathcal{A}(5)$ are not isomorphic to the multiplication group of any loop.

References


Received 1 July 1987 and in revised form 25 December 1988

ALES DRAPAL AND TOMÁŠ KEPKA
Department of Mathematics,
Charles University, Prague, Czechoslovakia