4-1958

On a Theorem of Hölder

Donald W. Miller
University of Nebraska - Lincoln

Follow this and additional works at: http://digitalcommons.unl.edu/mathfacpub

Part of the Mathematics Commons

Miller, Donald W., "On a Theorem of Hölder" (1958). Faculty Publications, Department of Mathematics. 45.
http://digitalcommons.unl.edu/mathfacpub/45

This Article is brought to you for free and open access by the Mathematics, Department of at DigitalCommons@University of Nebraska - Lincoln. It has been accepted for inclusion in Faculty Publications, Department of Mathematics by an authorized administrator of DigitalCommons@University of Nebraska - Lincoln.
ON A THEOREM OF HÖLDNER

DONALD W. MILLER, University of Wisconsin and University of Nebraska

1. Introduction. A well-known result, due to Höldner [1], is the following: The symmetric group \( S_n \) has outer automorphisms if and only if \( n=6 \). The classical proof of the existence of a class of outer automorphisms of \( S_6 \), as formulated by Burnside [2], rests in part on the theory of primitive groups and entails extensive computation. In this note we offer a direct method for constructing such automorphisms.

The author is grateful to Professor R. H. Bruck for raising this problem and for subsequent helpful remarks.

2. Construction of an outer automorphism of \( S_6 \). Let \( S_6 \) be defined on the set \( M = \{1, 2, 3, 4, 5, 6\} \); let \( I \) denote the identity of \( S_6 \). Call two elements of \( S_6 \) disjoint if no element of \( M \) is displaced by both of them.

Define the mapping \( \psi \) by:
\[
\begin{align*}
(1 2) & = (1 2)(3 6)(4 5) = P_3, \\
(1 3) & = (1 3)(2 4)(5 6) = P_4, \\
(1 4) & = (1 4)(2 6)(3 5) = P_5, \\
(1 5) & = (1 5)(2 3)(4 6) = P_6, \\
(1 6) & = (1 6)(2 5)(3 4) = P_6.
\end{align*}
\]
Write \( N = \{2, 3, 4, 5, 6\} \), \( \varphi = \{P_i | i \in N\} \). Note that the elements of \( \varphi \) include as factors the 15 distinct transpositions of \( S_6 \); consequently \( \varphi \) is transitive on \( M \). Moreover, for \( i, j, k \in M \), \( i \neq j \),
\[
P_i^2 = I, \quad kP_i \neq kP_j, \quad iP_j \neq i.
\]
Note that \( iP_j = jP_i \) implies \( i = j \). For if \( iP_j = jP_i = k \) then \( P_i = (1 i)(j k)(r s) \), \( P_j = (1 j)(i k)(r s) \), so \( i = j \). Also, \( P_iP_j = (i \ j \ jP_iP_j \ldots (1 \ i \ j \ P_iP_jP_j \ldots . \) Hence \( (jP_iP_j)P_jP_j \) equals \( i \) or \( 1 \). But in the latter case \( jP_iP_jP_j = jP_iP_i = P_6 \), whereas \( P_j \) fixes no element of \( M \). Thus \( P_iP_j \) has order three, so \( P_iP_jP_i = P_jP_iP_j \), all \( i, j \in N \).

If \( i, j, k \) are distinct elements of \( N \), then
\[
iP_j = jP_i = kP_j
\]
cannot hold. For, if so, write \( iP_j = q \) and \( N = \{i, j, k, q, r\} \). Now \( q = fP_r \) for some \( f \) in \( M \). Certainly \( f \) is not one of \( i, j, k, \) or \( q \). But if \( f = r \) then \( q = rP_r = 1 \), contradicting \( i \neq j \).

If \( P_i, P_j, P_k \) are distinct elements of \( \varphi \), then
\[
(P_iP_kP_j)P_i = P_j(P_iP_kP_j).
\]
It is sufficient to prove that \( P_k \) commutes with \( P_iP_kP_i \), for then \( P_kP_iP_iP_k = P_iP_kP_iP_iP_k = P_iP_kP_iP_kP_i = P_iP_kP_iP_kP_iP_k \), \( P_iP_kP_iP_k = P_iP_kP_iP_kP_iP_k \), \( P_iP_kP_i = P_iP_kP_iP_kP_iP_k \). Now
\[
Q = P_iP_kP_i = P_jP_iP_j = (1 \ iP_jP_i)(i \ jP_j)(j \ iP_j).
\]
Each of the three transpositions of \( Q \) is a factor of some \( P_k \), \( k \neq i, j \). If \( Q \) should have two cycles in common with some \( P_i \) then \( Q = P_i \). But in that case the dis-
played representation of $Q$ would yield $iP_j = jP_i$, $iP_i = t$ (so $iP_j = tP_i$), whence
$tP_i = iP_j = jP_i$, contradicting (1). (Thus we can write $Q = (a \ b)(c \ d)(e \ f)$, $P_k = (a \ b)(c \ f)(d \ e)$). But then $QP_k = (c \ e)(d \ f) = P_kQ$.

If $A_1, \ldots, A_n, B, C$ are distinct elements of $\varphi$, then

$$(3) \quad B(CA_1 \cdots A_nB) = (CA_1 \cdots A_nB)C.$$  

If $n = 1$, (3) follows from (2). Assume inductively that (3) holds for $n$; then

$B(CA_1 \cdots A_nA_{n+1}B)$
$= B(CA_1 \cdots A_nB)(BA_{n+1}B) = (CA_1 \cdots A_nBC)(A_{n+1}BA_{n+1})$
$= (CA_1 \cdots A_nA_{n+1})(BA_{n+1}BCA_{n+1})BA_{n+1} = (CA_1 \cdots A_nA_{n+1})(BCA_{n+1}B)BA_{n+1}$
$= (CA_1 \cdots A_nA_{n+1}B)C.$

Further, if $A_1, \ldots, A_n, B, C$ are distinct elements of $\varphi$, then

$$(4) \quad CB(A_1 \cdots A_n)B = B(A_1 \cdots A_n)BC.$$  

For by (3), $CBA_1 \cdots A_nB = BC(BCA_1 \cdots A_nB) = BC(CA_1 \cdots A_nBC) = B(A_1 \cdots A_nBC).$

Define the mapping $\theta$ as follows. Let $a_1, \ldots, a_n$ be distinct elements of $N$ and write $(1 \ a_i)\psi = A_i$. Then set

$$(5) \quad I\theta = I, \quad (1a_1 \cdots a_n)\theta = A_1 \cdots A_n,$$
$$(a_1a_2 \cdots a_n)\theta = A_nA_1A_2 \cdots A_n, \quad (QR)\theta = (Q\theta)(R\theta),$$

where $Q, R$ are arbitrary disjoint cycles of $S_6$. By (3),

$$(a_1a_2 \cdots a_n)\theta = A_1A_2 \cdots A_nA_1.$$  

Clearly $\theta$ maps $S_6$ into itself.

To show that $\theta$ is single-valued it will be sufficient to establish that if $Q = (a_1 \cdots a_m), R = (b_1 \cdots b_n)$ are arbitrary disjoint cycles in $S_6$, then

(i) $(QR)\theta = (RQ)\theta$;
(ii) $(a_1a_2 \cdots a_m)\theta = (a_2a_3 \cdots a_m a_1)\theta$.  

If $Q$ displaces 1 then $Q\theta$ is uniquely defined; if not, (ii) follows from (3). As to (i), suppose without loss of generality that $R$ does not displace 1; then $R\theta$ is of the form $BA_1 \cdots A_nB$, so by successive applications of (4), $(QR)\theta = (Q\theta)(R\theta)$
$= (R\theta)(Q\theta) = (RQ)\theta$.

For arbitrary elements $Q, R$ of $S_6$, $(QR)\theta = (Q\theta)(R\theta)$. To prove this it is sufficient to consider the case where $R$ is a transposition (since every element of $S_6$ is a product of transpositions). If $Q$ and $R$ are disjoint the asserted relation is trivial. Hence we write $Q$ as a product of disjoint cycles and let $Q'$ denote the product of those factors of $Q$ which are not disjoint from $R$. We need to show that $(Q'R)\theta = (Q\theta)(R\theta)$.

Let $1, e, f, a_1, \ldots, a_m, b_1, \ldots, b_n$ denote distinct elements of $M$.  

---

1958] ON A THEOREM OF HÖLDER 253
ON A THEOREM OF HÖLDER

(i) If \( Q' = (a_1 \cdots a_m), \quad R = (b_1), \) then \( (Q\theta)(R\theta) = A_1 \cdots A_mB_1 = (a_1 \cdots a_m b_1)\theta = (Q'R)\theta. \)

(ii) If \( Q' = (e a_1 \cdots a_m), \quad V = (e b_1 \cdots b_n), \) then \( (Q\theta)(V\theta) = (EA_1 \cdots A_mE)(EB_1 \cdots B_mE) = (e a_1 \cdots a_m b_1 \cdots b_n)\theta = (Q'V)\theta. \)

(iii) If \( Q' = (a_1 \cdots a_m e b_1 \cdots b_n), \quad R = (1 e), \) with \( m, n \geq 0, \) then \( (Q\theta)(R\theta) = A_1 \cdots A_m(EB_1 \cdots B_mE) = A_1 \cdots A_mB_nEB_1 \cdots B_n = [(1 a_1 \cdots a_m)
\cdot (e b_1 \cdots b_n)]\theta = (Q'R)\theta. \)

(iv) If \( Q' = (1 a_1 \cdots a_m)(e b_1 \cdots b_n), \quad R = (1 e), \) then \( (Q\theta)(R\theta) = A_1 \cdots A_mEB_1 \cdots B_mEE = A_1 \cdots A_mEB_1 \cdots B_n = (1 a_1 \cdots a_m e b_1 \cdots b_n)\theta = (Q'R)\theta. \)

(v) If \( Q' = (e a_1 \cdots a_m f b_1 \cdots b_n), \quad R = (e f), \) with \( m, n \geq 0, \) then by (4), \( (Q\theta)(R\theta) = (EA_1 \cdots A_mEFb_1 \cdots B_mE)(EFb_1 \cdots B_mE) = (EA_1 \cdots A_mE)(FB_1 \cdots B_mE)(EFb_1 \cdots B_mE) = (e a_1 \cdots a_m)(f b_1 \cdots b_n)\theta = (Q'R)\theta. \)

(vi) If \( Q' = (e a_1 \cdots a_m f b_1 \cdots b_n), \quad R = (e f), \) then, by (ii), \( (Q\theta)(R\theta) = (Q_1\theta)(Q_2\theta)(R\theta) = (Q_1\theta Q_2 R)\theta = (Q'R)\theta. \)

\( \theta \) is an automorphism of \( S_6. \) Indeed, the kernel, \( K, \) of \( \theta \) is a normal subgroup of \( S_6, \) so \( K \) is one of \( S_6, \) \( A_6, \) \( \{I\}, \) where \( A_6 \) denotes the alternating group of degree 6. But \( [(3 6)(4 5)]\theta = (3 6)(4 5), \) so \( K \not\cong S_6, \) \( K \not\cong A_6. \) Therefore \( K = \{I\} \) so \( \theta \) is 1-1 and hence an automorphism.

Finally, \( \theta \) is outer since \( (1 3 5)\theta = (1 2 6)(3 5 4), \) whereas if \( \theta \) were inner it would map every conjugate class of \( S_6 \) onto itself. This completes the proof.

We observe in conclusion that all outer automorphisms of \( S_6 \) are obtainable with the aid of the above construction. Indeed, as shown by Hölder [1], the automorphism group of \( S_6 \) has order 1440 = 2(6!); thus the group, \( S, \) of inner automorphisms is of index 2 in the full automorphism group. Hence if \( \theta \) is any outer automorphism of \( S_6 \) then the right coset \( 3\theta \) includes all outer automorphisms of \( S_6. \)

References