4-1958

# On a Theorem of Hölder

Donald W. Miller
*University of Nebraska - Lincoln*

The American Mathematical Monthly, Vol. 65, No. 4 (Apr., 1958), pp. 252-254


# ON A THEOREM OF HÖLDER

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

**1. Introduction.** A well-known result, due to Hölder [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: $(1\ 2)\psi=(1\ 2)(3\ 6)(4\ 5)=P_2$, $(1\ 3)\psi=(1\ 3)(2\ 4)(5\ 6)=P_3$, $(1\ 4)\psi=(1\ 4)(2\ 6)(3\ 5)=P_4$, $(1\ 5)\psi=(1\ 5)(2\ 3)(4\ 6)=P_5$, $(1\ 6)\psi=(1\ 6)(2\ 5)(3\ 4)=P_6$. Write $N=\{2, 3, 4, 5, 6\}$, $\mathcal{P}=\{P_i \mid i\in N\}$. Note that the elements of $\mathcal{P}$ include as factors the 15 distinct transpositions of $S_6$; consequently $\mathcal{P}$ is transitive on $M$. Moreover, for $i, j, k\in M$, $i\neq j$,

$$P_i^2 = I, \qquad kP_i \neq kP_j, \qquad iP_j \neq i.$$

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, $P_iP_j=(i\ \ j\ \ jP_iP_j\ \cdots (1\ \ iP_j\ \ iP_jP_iP_j \cdots$. Hence $(jP_iP_j)P_iP_j$ equals $i$ or 1. But in the latter case $jP_iP_j=1P_jP_i=jP_i$, 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

$$iP_j = jP_k = kP_i \tag{1}$$

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 $\mathcal{P}$, then

$$(P_iP_kP_j)P_i = P_j(P_iP_kP_j). \tag{2}$$

It is sufficient to prove that $P_k$ commutes with $P_iP_jP_i$, for then $P_kP_iP_jP_i = P_iP_jP_iP_k$, $P_iP_kP_iP_jP_i = P_jP_iP_k$, $P_iP_kP_jP_iP_j = P_jP_iP_kP_jP_j$, $P_iP_kP_jP_i = P_jP_iP_kP_j$. Now

$$Q = P_iP_jP_i = P_jP_iP_j = (1\ \ iP_jP_i)(i\ \ jP_i)(j\ \ iP_j).$$

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 $P_t$ then $Q=P_t$. But in that case the displayed representation of $Q$ would yield $iP_j = jP_t$, $iP_jP_i = t$ (so $iP_j = tP_i$), whence $tP_t = iP_j = jP_t$, 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 $A_1, \cdots, A_n, B, C$ are distinct elements of $\mathcal{P}$, then

$$B(CA_1 \cdots A_nB) = (CA_1 \cdots A_nB)C. \tag{3}$$

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

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

Further, if $A_1, \cdots, A_n, B, C$ are distinct elements of $\mathcal{P}$, then

$$CB(A_1 \cdots A_n)B = B(A_1 \cdots A_n)BC. \tag{4}$$

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 $a_1, \cdots, a_n$ be distinct elements of $N$ and write $(1\ a_i)\psi = A_i$. Then set

$$\begin{aligned} I\theta = I, \qquad (1a_1 \cdots a_n)\theta = A_1 \cdots A_n, \\ (a_1a_2 \cdots a_n)\theta = A_nA_1A_2 \cdots A_n, \qquad (QR)\theta = (Q\theta)(R\theta), \end{aligned} \tag{5}$$

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) $(a_1a_2 \cdots a_m)\theta = (a_2a_3 \cdots a_ma_1)\theta$.

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

(i) If $Q' = (1\ a_1 \cdots a_m)$, $R = (1\ b_1)$, then $(Q'\theta)(R\theta) = A_1 \cdots A_m B_1 = (1\ a_1 \cdots a_m\ b_1)\theta = (Q'R)\theta$.

(ii) If $Q' = (e\ a_1 \cdots a_m)$, $V = (e\ b_1 \cdots b_n)$, then $(Q'\theta)(V\theta) = (EA_1 \cdots A_m E) \cdot (EB_1 \cdots B_n E) = EA_1 \cdots A_m B_1 \cdots B_n E = (e\ a_1 \cdots a_m\ b_1 \cdots b_n)\theta = (Q'V)\theta$.

(iii) If $Q' = (1\ a_1 \cdots a_m\ e\ b_1 \cdots b_n)$, $R = (1\ e)$, with $m, n \geqq 0$, then $(Q'\theta)(R\theta) = A_1 \cdots A_m(EB_1 \cdots B_n E) = A_1 \cdots A_m B_n E B_1 \cdots B_n = [(1\ a_1 \cdots a_m) \cdot (e\ b_1 \cdots b_n)]\theta = (Q'R)\theta$.

(iv) If $Q' = (1\ a_1 \cdots a_m)(e\ b_1 \cdots b_n)$, $R = (1\ e)$, then $(Q'\theta)(R\theta) = A_1 \cdots A_m E B_1 \cdots B_n E E = A_1 \cdots A_m E B_1 \cdots B_n = (1\ a_1 \cdots a_m\ e\ b_1 \cdots b_n)\theta = (Q'R)\theta$.

(v) If $Q' = (e\ a_1 \cdots a_m\ f\ b_1 \cdots b_n)$, $R = (e\ f)$, with $m, n \geqq 0$, then by (4), $(Q'\theta)(R\theta) = (EA_1 \cdots A_m F B_1 \cdots B_n E)(EFE) = (EA_1 \cdots A_m)(FB_1 \cdots B_n FE) = (EA_1 \cdots A_m)(EFB_1 \cdots B_n F) = [(e\ a_1 \cdots a_m)(f\ b_1 \cdots b_n)]\theta = (Q'R)\theta$.

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

$\theta$ 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 $K \neq S_6$, $K \neq A_6$. 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, $\mathfrak{J}$, 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 $\mathfrak{J}\theta$ includes all outer automorphisms of $S_6$.

### References


1. O. Hölder, Bildung zusammengesetzter Gruppen, Math. Ann., vol. 46, 1895, pp. 321–422.
2. W. Burnside, Theory of Groups of Finite Order, Cambridge, 1911.