THE AUTOMORPHISMS OF THE SYMMETRIC GROUP

IRVING E. SEGAL

The purpose of this note is to give a proof of the following well known theorem. *The group of automorphisms of the symmetric group S_n on n letters is isomorphic with S_n, except when $n=6$.* The proofs of this in the literature are complicated[1] and involve the use of lemmas whose relevance is not plain.

Let A be an automorphism of S_n. Then it is clear that A takes a class of similar elements into a class of similar elements, and that it takes an element of order m into an element with the same order. Hence suppose $A(1r)=t_1(r)\cdot t_2(r)\cdot \cdots \cdot t_k(r)$ $(k\geqq 1)$, where the $t_i(r)$ are disjoint transpositions. A simple calculation shows that there are $n(n-1)/2$ elements similar to $(1r)$, and that there are $n!/2^k k!(n-2k)!$ elements similar to $t_1(r)\cdot t_2(r)\cdot \cdots \cdot t_k(r)$. Hence

$$\frac{n(n-1)}{2}=\frac{n!}{2^k k!(n-2k)!}.$$

If $n\neq 6$ this equation is satisfied for no k $(k\geqq 1)$ except $k=1$.

Suppose now that $n\neq 6$. Then $A(1r)=(a_rb_r)$ say. If $r\neq 2$, $(12)(1r)=(12r)$ (multiplying from right to left), and evidently, $A(12r)=(a_2b_2)(a_rb_r)$. Since $(12r)$ has the order 3, so has $(a_2b_2)(a_rb_r)$ and the transpositions (a_2b_2) and (a_rb_r) must have a letter in common. Then it is no loss to assume $a_2=a_r$ or $b_2=b_r$. However, if $a_2=a_r$ and $b_2=b_s$ $(r\neq 2,\ s\neq 2)$, then $r\neq s$ and $A(12r)=A(12)\cdot A(1r)=(a_2b_2)(a_2b_r)=(b_ra_2b_2)$. Similarly $A(12s)=(a_sb_2a_2)$. Hence $A((12r)\cdot(12s))=A(12r)\cdot A(12s)=(b_ra_2b_2)(a_sb_2a_2)=(b_ra_sb_2)$ which is of order 3, while $(12r)\cdot(12s)=(1s)(2r)$, which is of order 2. Hence one must have $a_2=a_r$ for all r or $b_2=b_r$ for all r; of course one can let $a_2=a_r$ $(r=2,3,\cdots,n)$. Then $A(1r)=(a_2b_r)$. Hence A is precisely the automorphism A defined by $Ax=t^{-1}xt$, where

$$t=\begin{pmatrix}1 & 2 & \cdots & r & \cdots & n\\ a_2 & b_2 & \cdots & b_r & \cdots & b_n\end{pmatrix}.$$

For $Ax=t^{-1}xt$ when $x=(1r)$, and the elements $\{(1r)\}$ $(r=2,3,\cdots,n)$ generate S_n.

YALE UNIVERSITY

[1] The first proof is by O. Hölder, Mathematische Annalen, vol. 46 (1895), especially pp. 340–345.