Cauchy on Permutations and the Theory of Equations

As discussed in the text, Ruffini had shown that it was not possible to exhibit a function of five variables that could be changed into three different functions or four different functions by permuting the variables. It was this work that Cauchy generalized. We give here some mathematical details that had to be left out of the text itself.

Cauchy showed how to write any permutation of order 3 as the composition of two permutations of order p.* The technique was quite simple. If $\alpha \to \beta \to \gamma \to \alpha$ is the permutation of order 3, introduce $p - 3$ other elements $\delta, \varepsilon, \ldots, \zeta, \eta$, and let the permutations be

$$\alpha \to \gamma \to \beta \to \delta \to \varepsilon \to \cdots \to \zeta \to \eta \to \alpha$$

and

$$\alpha \to \eta \to \zeta \to \cdots \to \varepsilon \to \delta \to \gamma \to \beta \to \alpha$$

It is easy to see that the effect of carrying out these operations in this order is the cyclic permutation $\alpha \to \beta \to \gamma \to \alpha$, all other elements being left fixed.

But, once it is given that all cyclic permutations of order three leave the function invariant, it follows that the effect of all simple transposition $\alpha \to \beta \to \alpha$ must be the same. For it is obvious that such a transposition is its own inverse, and hence produces at most two different functions when it is applied repeatedly. Its composition with the transposition $\beta \to \gamma \to \beta$ is a cycle of order three, namely $\alpha \to \gamma \to \beta \to \alpha$, and hence must leave the function invariant. Therefore the two functions that the first transposition interchanges must also be interchanged by the second one. Finally, since the effect of $\alpha \to \beta \to \alpha$ is the same as the effect of $\beta \to \gamma \to \beta$, which is the same as the effect of $\gamma \to \delta \to \gamma$, and so on, it follows that all simple transpositions have the same effect. Hence the permutation group can produce at most two different functions. For this case Cauchy showed that the function must be of the form $K + SV$, where K and S are symmetric and V is the Vandermonde determinant mentioned above, which switches sign when any two of its arguments are permuted.

Besides the notation for permutations and cycles, Cauchy also invented some of the terminology of group theory, including the word *index* (*indice*) still used for the number of cosets of a subgroup of a finite group. For the number of elements M in the subgroup, he used the term *indicial (or indicative) divisor* (*diviseur indicatif*). He proposed the name *substitution* (of one permutation into another) for the composition of two permutations, and to call two permutations *equivalent* if they produce the same function, that is, they are equal modulo the subgroup of permutations that leave the function invariant. To picture cyclic permutations of finite order, he suggested arranging the distinct powers as the vertices of a regular polygons and thinking of the composition of two of them as a clockwise rotation (he said "a rotation from east to west") of the polygon. Such an arrangement suggests studying the symmetries of these polygons. However, although he frequently referred to "groups of indices" in this paper, he did not define the notion of a group in its modern sense. We can see that he was using group properties for the special case of the symmetric group on n letters, but he did not give any formal definitions, except for the terms just listed.

* The number $N = n!$ has no prime factors larger than n, so that $p \le n$ in any case.