L'Enseignement Mathématique, t. 38 (1992), p. 41-53

PERMUTATION GROUPS GENERATED BY A TRANSPOSITION AND ANOTHER ELEMENT

by Gerald J. JANUSZ

ABSTRACT: The subgroup of the symmetric group Sym(n) generated by a transposition and another element is described explicitly using data easily obtained from the two elements. The proofs use a graph that is defined for any subgroup of Sym(n) that contains a transposition. Application is made to prove that a rational, irreducible polynomial of degree n having exactly $n - 2$ real roots is not solvable by radicals provided that n is not divisible by 2 or 3.

In the begining study of the symmetric group Sym(Ω) of all permutations on a set Ω the student learns the standard fact that every permutation can be expressed as a product of transpositions; otherwise put, Sym(Ω) is generated by its transpositions. In some expositions, other generating sets are mentioned. For example for a prime p, it is not difficult to show that the symmetric group Sym(p) on p symbols is generated by a p-cycle and a transposition. In fact any p-cycle and any transposition will generate Sym(p).

A well-known theorem of Galois theory folklore (see [1, Theorem 4.16]) uses this information about the generation of the symmetric group to prove the existence of polynomials not solvable by radicals. In this theorem one considers a polynomial $f(x)$ of prime degree $p \geqslant 5$ having rational coefficients. Assume that $f(x)$ is irreducible over the rational numbers and has exactly $p - 2$ real roots. Then the Galois group of the splitting field of $f(x)$ over the rational field is not solvable. In fact the Galois group is isomorphic to the symmetric group on p symbols. In particular the polynomial is not solvable by radicals. Here is a sketch of the proof. When the Galois group is regarded as a permutation group on the p roots of $f(x)$, the hypothesis implies that the Galois group contains a p-cycle and a transposition and hence it must be the full symmetric group on the p roots.

This proof breaks down for nonprime degree. If n is not prime, an n-cycle may be paired with a transposition in Sym(n) to generate a subgroup smaller

1991 Mathematics Subject Classification: primary 20B30; secondary 12E05, 12F10.