2. An application to Galois theory

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **38 (1992)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

COROLLARY 2 (C. Jordan [3]). *A primitive subgroup of* $\mathrm{Sym}(n)$ *containing a transposition is all of* $\mathrm{Sym}(n)$.

Proof. Let $\mathscr{H}$ be a primitive subgroup of $\mathrm{Sym}(n)$ and τ a transposition in $\mathscr{H}$. Then $\mathscr{H}$ permutes the components Γ_i of $\Gamma(\mathscr{H}, \tau)$ and so the vertex sets V_i of the Γ_i are permuted by $\mathscr{H}$. The primitivity of $\mathscr{H}$ implies that the set $\{1, 2, \cdots, n\}$ can be partitioned into disjoint subsets permuted by $\mathscr{H}$ only if each subset has order one or there is just one subset of order n. Since the vertex set of Γ_i has more than one element, there is only one component and $\mathscr{H} = \mathrm{Sym}(n)$ by Corollary 1.

2. AN APPLICATION TO GALOIS THEORY

We extend the theorem mentioned in the introduction replacing the condition that the degree of the polynomial be a prime greater than 3 by the condition that the degree of the polynomial be divisible only by primes greater than 3.

THEOREM 2. *Left* $f(x)$ *be a polynomial of degree* n *with rational coefficients and irreducible over the rational field. Assume that* $f(x)$ *has exactly* $n - 2$ *real roots. If* n *is divisible only by primes greater than 3 then the Galois group of the splitting field of* $f(x)$ *is not solvable and* $f(x)$ *is not solvable by radicals.*

Proof. Let $\mathscr{H}$ be the Galois group of $f(x)$ over the rational field. We view $\mathscr{H}$ as a permutation group on the n roots of f. Then complex conjugation, τ, is a transposition in $\mathscr{H}$ of the two nonreal roots. Since $f(x)$ is irreducible, $\mathscr{H}$ is transitive on the set of n roots. By theorem 1, $\mathscr{H}$ contains a subgroup isomorphic to the direct product of t copies of $\mathrm{Sym}(k)$ where $tk = n$. Since k is a divisor of n and $k > 1$, the hypothesis on the divisors of n implies $k \geqslant 5$. Thus $\mathrm{Sym}(k)$ is not a solvable group and $\mathscr{H}$ is not solvable as it contains a nonsolvable subgroup. Thus $f(x)$ is not solvable by radicals.

3. TWO GENERATOR SUBGROUPS OF $\mathrm{Sym}(n)$

Next we apply Theorem 1 to determine the subgroup of $\mathrm{Sym}(n)$ generated by a transposition and one other element. We first consider the case in which