than Sym(n) (see Corollary 5). The simplest example is the group of order 8 generated by (1, 2, 3 ,4) and (1, 3) having index 3 in Sym(4).

The object of this note is to show how the subgroup of Sym(n) generated by a transposition and one other element can be determined. In particular we will define a graph associated with a cycle σ and a transposition τ. (In fact the graph will be defined for a somewhat more general situation.) An easily computable condition on σ and τ (or on the graph) will determine if the group generated by σ and τ is the full symmetric group. To show that a wide variety of groups can be generated by a transposition and a cycle, we mention three cases. Let $\sigma = (1, 2, 3, 4, 5, 6, 7, 8)$ and τ one of the 28 transpositions in Sym(8). Then the subgroup of Sym(8) generated by σ and τ is all of Sym(8), a group of order 40320, for 16 choices of τ; is a group of order 1152 for 8 choices of τ and a group of order 64 for 4 choices of τ.

Once the case of an n-cycle and a transposition has been done, it is fairly straight forward to do the general case. We determine the group generated by a transposition and any other element. As an application of these ideas we show that the theorem on Galois groups mentioned above remains valid for polynomials of degree n not divisible by 2 or 3.

1. A GRAPH FOR A SUBGROUP CONTAINING A TRANSPOSITION

We consider a subgroup $\mathscr{H}$ of Sym(n) that contains a transposition $\tau = (a, b)$. We will define a graph depending on $\mathscr{H}$ and τ and use it to prove the existence of a normal subgroup of $\mathscr{H}$ whose structure can be described explicitly.

Let $\Gamma = \Gamma(\mathscr{H}, \tau)$ be the graph whose vertex set is $V = \{1, 2, \cdots, n\}$ on which $\mathscr{H}$ acts as permutations. An edge of Γ is a two element subset $\{i, j\}$ of vertices such that the transposition (i, j) is conjugate to τ in $\mathscr{H}$. Thus $\{i, j\}$ is an edge of Γ if and only if there is some element $\eta \in \mathscr{H}$ such that

$$\eta\tau\eta^{-1} = (i, j) .$$

For any transposition (r, s) we have

$$\eta(r, s)\eta^{-1} = (\eta(r), \eta(s)) \tag{1}$$

so it follows that $\{i, j\}$ is an edge of Γ if and only if $\{i, j\} = \{\eta(a), \eta(b)\}$ for some $\eta \in \mathscr{H}$. The action of $\mathscr{H}$ on the vertices of Γ permutes the edges and so $\mathscr{H}$ is part of the automorphism group of Γ. The notion of a path and

connected vertices will be used to examine the structure of $\mathscr{H}$. We remind the reader of the relevant concepts associated with the graph.

A *path* in Γ is a sequence of edges such that adjacent terms of the sequence have a vertex in common. Two vertices u and v are *connected* if there is a path in Γ with u and v vertices of some edges in the path. A *component* of Γ is a maximal subgraph in which any two vertices are connected by a path. It is easy to see that connectedness is an equivalence relation on the set of vertices and so the vertex set V is partitioned into disjoint subsets $V_1, \cdots, V_t$ maximal with the property that two vertices in a subset are connected. Then Γ is a disjoint union

$$\Gamma = \Gamma_1 \cup \Gamma_2 \cup \cdots \cup \Gamma_t , \quad t \geqslant 1 ,$$

with each Γ_i a component of Γ.

We now show that each component is a complete graph on its vertices; *i.e.* every pair of vertices of Γ_i lie on an edge. Let i and j be two vertices connected by a path in Γ. Then there are transpositions

$$\tau_1 = (i, a_1) , \quad \tau_2 = (a_1, a_2) , \cdots, \tau_r = (a_{r-1}, a_r) , \cdots, \tau_k = (a_{k-1}, j)$$

in $\mathscr{H}$ and each is conjugate to τ. Then each of the following transpositions is in $\mathscr{H}$ and is also conjugate to τ:

$$\begin{aligned} \tau_2\tau_1\tau_2 &= (i, a_2) , \\ \tau_3(i, a_2)\tau_3 &= (i, a_3) , \\ \tau_4(i, a_3)\tau_4 &= (i, a_4) , \\ &\cdots\cdots\cdots \\ \tau_k(i, a_{k-1})\tau_k &= (i, j) . \end{aligned}$$

Thus $(i, j) \in \mathscr{H}$ and there is an edge of Γ connecting i and j. In other words this argument shows that $\mathscr{H}$ contains every transposition of $\mathrm{Sym}(n)$ that exchanges a pair of connected vertices. This gives the information needed in the following statement:

THEOREM 1. *Let $\mathscr{H}$ be a subgroup of the symmetric group $\mathrm{Sym}(n)$; assume $\mathscr{H}$ contains a transposition τ. Let the components of the graph $\Gamma(\mathscr{H}, \tau)$ be $\Gamma_1, \cdots, \Gamma_t$ and let V_i denote the set of vertices of Γ_i. Let S be the subgroup of $\mathscr{H}$ generated by all the conjugates of τ in $\mathscr{H}$. Then S is a normal subgroup of $\mathscr{H}$ and is isomorphic to the direct product $S_1 \times \cdots \times S_t$ where S_i is the symmetric group of all permutations of V_i.*

Assume $\mathscr{H}$ *is transitive on* $\{1, 2, \cdots, n\}$. *Then the groups* $S_1, \cdots, S_t$ *are isomorphic and* S *is isomorphic to* $\mathrm{Sym}(k)^{(t)}$, *the direct product of* t *copies of* $\mathrm{Sym}(k)$ *where* $tk = n$ *and* $k > 1$. *The elements of* $\mathscr{H}$ *permute the components* $\Gamma_1, \cdots, \Gamma_t$ *and only the elements of* S *leave all the* Γ_i *fixed (as sets). Thus* $\mathscr{H}/S$ *is isomorphic to a transitive subgroup of* $\mathrm{Sym}(t)$.

Proof. The statement that S is a normal subgroup of $\mathscr{H}$ follows at once because the set of generators of S is closed under conjugation by elements of $\mathscr{H}$. The conjugate class of τ consists of transpositions corresponding one-to-one with the edges of Γ. Let S_i be the subgroup generated by the transpositions corresponding to edges of Γ_i. Since we have seen that Γ_i has an edge joining every pair of vertices, S_i contains every transposition permuting two elements of V_i. Thus S_i is the full symmetric group $\mathrm{Sym}(V_i)$ of permutations of V_i. Since the S_i permute disjoint sets of vertices, the group S is the direct product of the groups $S_1, \cdots, S_t$.

Now suppose that $\mathscr{H}$ is transitive on V. For any pair of indices i and j and verticies $u \in \Gamma_i$ and $v \in \Gamma_j$, there is an element $\eta \in \mathscr{H}$ with $\eta(u) = v$. It follows that $\eta(\Gamma_i) = \Gamma_j$, $\eta(V_i) = V_j$ and $\eta S_i \eta^{-1} = S_j$. So any two of the groups $S_1, \cdots, S_t$ are conjugate, hence isomorphic. If k is the number of vertices of Γ_i (for any i) then

$$S = S_1 \times \cdots \times S_t \cong \mathrm{Sym}(k) \times \cdots \times \mathrm{Sym}(k) = \mathrm{Sym}(k)^{(t)} .$$

Because k is the number of vertices in each Γ_i, and since Γ_i contains at least one edge, Γ_i must contain at least two vertices. Thus $k \geqslant 2$.

We have already seen that $\mathscr{H}$ permutes the set $\{\Gamma_1, \cdots, \Gamma_t\}$ of components; the elements in S leave each Γ_i fixed because S_j is generated by transpositions which leave every Γ_i fixed. We will now prove that the only elements of $\mathscr{H}$ that leave every Γ_i fixed are the elements of S. Suppose $\eta \in \mathscr{H}$ and $\eta(\Gamma_i) = \Gamma_i$ for $1 \leqslant i \leqslant t$. Then $\eta S_i \eta^{-1} = S_i$; conjugation by η induces an automorphism of S_i. A great deal is known about the automorphisms of symmetric groups. An automorphism of $\mathrm{Sym}(k)$ is a conjugation by an element of $\mathrm{Sym}(k)$ except possibly when $k = 6$ (see [4, Theorem 7.4, page 133]). An automorphism of $\mathrm{Sym}(6)$ is either a conjugation by an element of $\mathrm{Sym}(6)$ or it has the property that every transposition is mapped to the product of three transpositions (see [2]). In the present case, the automorphism $\lambda \to \eta\lambda\eta^{-1}$ must send transpositions to transpositions. Hence there is an element $\gamma_i \in S_i$ such that $\eta\lambda\eta^{-1} = \gamma_i^{-1}\lambda\gamma_i$ for all $\lambda \in S_i$. The elements of different S_i commute with each other so it follows that

$$\gamma_1 \cdots \gamma_t \eta \lambda \eta^{-1} (\gamma_1 \cdots \gamma_t)^{-1} = \lambda$$

for every $\lambda \in S_i$ and for every i. The element $\alpha = \gamma_1 \cdots \gamma_t \eta$ commutes with every element of S; in particular α commutes with every transposition in S. In view of Equation (1), an element centralizing each transposition must leave every edge of Γ fixed. There are only two possibilities for an automorphism of Γ that fixes all edges. If there is a path in Γ with two or more edges, then every edge lies on a path with two or more edges (because the components are complete graphs and two components are isomorphic). In this case the only automorphism fixing every edge is the identity on the vertices. Thus in this case $\gamma_i \cdots \gamma_t \eta = e$ and $\eta \in S$.

In the remaining case there are no paths of length two in Γ and so every S_i is of order 2. The element α leaves every edge fixed and so either fixes or permutes the two vertices of Γ_i. If $S_i = \langle (u, v) \rangle$ and if α moves u then α must interchange u and v because edges are preserved. It follows that $(u, v)\alpha$ fixes u and v. By repeating this argument for each component of Γ we get α multiplied by certain transpositions in S leaves all vertices fixed and hence is the identity. It follows that η is the product of the transpositions in certain of the S_i. Thus in this case we also have $\eta \in S$ and the only elements of $\mathscr{H}$ fixing the sets V_i are the elements of S. Thus the group of permutations of the Γ_i induced by the action of $\mathscr{H}$ is the group $\mathscr{H}/S$. So $\mathscr{H}/S$ is isomorphic to a subgroup of $\mathrm{Sym}(t)$. Note that if $\mathscr{H}$ acts transitively on $\{1, 2, \cdots, n\}$, then $\mathscr{H}/S$ acts transitively on $\{\Gamma_1, \cdots, \Gamma_t\}$.

The graph $\Gamma(\mathscr{H}, \tau)$ can be used to give an easy criterion to determine when $\mathscr{H} = \mathrm{Sym}(n)$.

COROLLARY 1. *The subgroup of* $\mathrm{Sym}(n)$ *generated by a subgroup* $\mathscr{H}$ *containing a transposition* τ *is all of* $\mathrm{Sym}(n)$ *if and only if the graph* $\Gamma(\mathscr{H}, \tau)$ *is connected.*

Proof. If $\Gamma(\mathscr{H}, \tau)$ is connected then $\mathscr{H}$ contains every transposition (i, j) because the graph is a complete graph containing every possible edge, as shown earlier. Since every permutation in $\mathrm{Sym}(n)$ is a product of transpositions, and all the transpositions are in $\mathscr{H}$, it follows that $\mathscr{H} = \mathrm{Sym}(n)$. Conversely if $\mathscr{H} = \mathrm{Sym}(n)$, then every transposition in $\mathscr{H}$ is conjugate to τ and the graph $\Gamma(\mathscr{H}, \tau)$ contains every possible edge; in particular the graph is connected.

The graph Γ provides a tool that enables us to give a quick proof of a special case of a theorem first proved by C. Jordan.

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