3. TWO GENERATOR SUBGROUPS OF Sym(n)

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **23.07.2024**

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 the other element is an n-cycle. Let $\sigma = (1, 2, \cdots, n)$ and $\tau = (a, b)$ with $1 \leqslant a < b \leqslant n$ and let $G = \langle \sigma, \tau \rangle$ be the group generated by the two elements. Then G is transitive on $\{1, 2, \cdots, n\}$ because the cyclic subgroup $\langle \sigma \rangle$ is transitive. Theorem 1 will be applied to prove the following result.

THEOREM 3. *Let σ be an n-cycle and $\tau = (a, b)$ a transposition in* $\mathrm{Sym}(n)$ *and G the subgroup of* $\mathrm{Sym}(n)$ *generated by σ and τ. Let q be a positive integer such that $\sigma^q(a) = b$ and let $t = gcd(n, q)$. Then t is the least positive integer such that τ and $\sigma^t\tau\sigma^{-t}$ correspond to edges in the same connected component of the graph $\Gamma(G, \tau)$ defined above. If we write $n = tk$ for some integer k then G contains a normal subgroup S isomorphic to the direct product of t copies of* $\mathrm{Sym}(k)$. *The quotient G/S is cyclic of order t. In particular G is a solvable group if and only if $k \leqslant 4$.*

Proof. Let S be the subgroup of G generated by all the transpositions conjugate in G to τ. By Theorem 1, S is the direct product of t copies of $\mathrm{Sym}(k)$ where t is the number of components of the graph $\Gamma(G, \tau)$. Let $\Gamma_1, \cdots, \Gamma_t$ be the components of $\Gamma(G, \tau)$. Since σ is an n-cycle, the cyclic group $\langle \sigma \rangle$ permutes the components transitively. It follows that σ^t fixes each Γ_i and so $\sigma^t \in S$ and no smaller positive power of σ fixes any one of the Γ_i. Thus t is the least positive integer such that the edges corresponding to τ and $\sigma^t\tau\sigma^{-t}$ lie in the same component of $\Gamma(G, \tau)$. The fact that G/S is cyclic follows from the fact that G is generated by σ and τ and τ is in S. Thus G/S is generated by the coset σS.

The group G is solvable if and only if S and G/S are solvable; G/S is cyclic, hence solvable. S is solvable if and only if $\mathrm{Sym}(k)$ is solvable. It is well known that $\mathrm{Sym}(k)$ is solvable if and only if $k \leqslant 4$.

We must now show that t is obtained as stated. We make a change of notation to facilitate the proof. Let R denote the ring $Z/(n)$ of integers modulo n and view $\mathrm{Sym}(n)$ as a group of permutations of R. By renaming the elements, we may assume that σ is the n-cycle defined by $\sigma(x) = x + 1$ (with the addition in R used, of course). Let $\tau = (a, b)$ with $a, b \in R$ and take $q = b - a$. Since $\sigma^q(a) = a + q = b$, any other integer power of σ that carries a to b will have exponent congruent modulo n to $b - a$ so there is no harm in assuming $q = b - a$.

Let $G = \langle \sigma, \tau \rangle$; we will show that the connected components of the graph $\Gamma(G, \tau)$ have the cosets $x + qR$ as the vertex sets. The case in which qR has only two elements is somewhat exceptional and easy so we treat it first. When qR has two elements then n is even and $q \equiv n/2 \pmod{n}$ and

$$a + qR = a + (b - a)R = \{a, b\}.$$

Thus τ fixes every coset $x + qR$ and σ carries $x + qR$ to $x + 1 + qR$. Thus the edges of $\Gamma(G, \tau)$ are the pairs in the distinct cosets and each connected component consists of two vertices and one edge. There are $n/2$ components and so the number t of Theorem 3 is $t = n/2$ which equals $gcd(n, q)$ as required.

Let r be the number of elements in qR and now assume $r > 2$. Thus $r = n/gcd(n,q)$ and $rq = 0$ in R. The elements in a coset $u + qR$ have the form $u + jq$, with $1 \leqslant j \leqslant r$. The cosets are permuted transitively by $\langle \sigma \rangle$. Each coset is left invariant by τ. This is clear for cosets not containing a or b. Since $a + q = b$, both a and b lie in $a + qR$ so τ also leaves $a + qR$ invariant. The edges of Γ are generated by applying the elements of G to the edge $\{a, b\}$. Thus the endpoints of an edge of Γ lie in the same coset of qR. Hence a connected component has all its vertices in one coset and thus a component has at most r vertices. Now we show that all vertices in a coset are connected. It is sufficient to show this for the coset $a + qR$ since G is transitive on the components. The following computation is crucial for this verification:

$$(2) \qquad (\tau\sigma^q)^j\{a, b\} = \{a, b + jq\} \quad \text{for} \quad 1 \leqslant j \leqslant r - 2\,.$$

We verify this by induction on j. For $j = 1$ we have

$$\tau\sigma^q\{a, b\} = \tau\{a + q, b + q\} = \tau\{b, b + q\}.$$

If we had $b + q = a$, then $0 = b - a + q = 2q$ and it follows that qR has only two elements. In the present case we have $r > 2$ so $b + q \neq a$ and $\tau(b + q) = b + q$. Since $\tau(b) = a$ we see that (2) holds for $j = 1$. Now assume (2) holds for j and that $j + 1 \leqslant r - 2$. Then

$$\begin{aligned}(\tau\sigma^q)^{j+1}\{a, b\} &= \tau\sigma^q\{a, b + jq\}\\ &= \tau\{a + q, b + (j + 1)q\}\\ &= \tau\{b, b + (j + 1)q\}.\end{aligned}$$

If $b + (j + 1)q = a$ then $(j + 2)q = 0$. This implies $j + 2 \geqslant r$ contrary to the choices of j. Thus $\tau(b + (j + 1)q) = b + (j+1)q$ and $\tau(b) = a$; thus (2) holds.

This computation shows that there are $r - 2$ edges connecting a to verticies $b + jq$. The edge $\{a, b\}$ is not counted among these. Thus we account for $r - 1$ edges containing a and r vertices in the connected component containing a. We have already seen that the components contain no more than r vertices. Hence there are exactly $r = n/gcd(n, q)$ vertices in a component and the number of components is $n/r = gcd(n, q)$ as we wanted to prove.

The group $\langle \sigma, \tau \rangle$ equals Sym(n) precisely when the graph Γ has just one component, that is $t = 1$ in Theorem 3. We have the following easily applied criterion.

COROLLARY 4. *Let σ be an n-cycle and $\tau = (a, b)$ a transposition in* Sym(n). *Let q be an integer such that $\sigma^q(a) = b$. Then the group generated by σ and τ is all of* Sym(n) *if and only if $gcd(n, q) = 1$.*

We give two examples that determine the two generator groups using Theorem 3.

Example 1. Let $\sigma = (1, 2, 3, 4, 5, 6, 7, 8)$ and $\tau = (1, 5)$. The description of $\Gamma = \Gamma(\langle \sigma, \tau \rangle, \tau)$ may be obtained using Theorem 3. Since $\sigma^4(1) = 5$ we find there are $t = gcd(8, 4) = 4$ components with 2 vertices in each.

In order to determine the group $G = \langle \sigma, \tau \rangle$ explicitly, we find the component of Γ. We find the edges of Γ by repeatedly applying σ to the edge $\{1, 5\}$ to obtain the edges

$$\{2, 6\}, \{3, 7\}, \{4, 8\}, \{1, 5\}.$$

Application of τ does not yield any new edges and so these are all the edges in Γ. The groups of permutations of the components are:

$$S_1 = \langle (2, 6) \rangle, \quad S_2 = \langle (3, 7) \rangle, \quad S_3 = \langle (4, 8) \rangle, \quad S_4 = \langle (1, 5) \rangle.$$

The conjugation action of σ is to cyclically permute the factors S_1, S_2, S_3, S_4 and $\sigma^4 = (1, 5)(2, 6)(3, 7)(4, 8)$ is in $S_1 \times \cdots \times S_4$. Thus the order of G is

$$|S_1|^4 \, |\langle \sigma \rangle / \langle \sigma^4 \rangle| = 2^4 \cdot 4 = 64 .$$

Example 2. Let $\sigma = (1, 2, 3, 4, 5, 6, 7, 8)$ and $\tau = (1, 6)$. Since $\sigma^5(1) = 6$ and $gcd(8, 5) = 1$, Corollary 4 implies $\langle \sigma, \tau \rangle = \text{Sym}(8)$.

Now we consider the description of $\langle \sigma, \tau \rangle$ with τ a transposition and σ any element of Sym(n), not necessarily an n-cycle. The discussion will be broken into cases depending on how σ and τ are realted.

To make the notation simpler, let us assume $\tau = (1, 2)$. We may express σ as a product of disjoint cycles

$$\sigma = \xi_1 \xi_2 \cdots \xi_r, \qquad \xi_j \text{ a cycle} .$$

Let V_i be the set of symbols moved by ξ_i so that ξ_i permutes the elements of V_i transitively and fixes the elements of V_j for $j \neq i$.

The first case in which σ is a cycle and τ is a transposition moving two symbols that are also moved by σ is covered in Theorem 3.

Second case. $1, 2 \in V_1$. This is the case in which the two elements moved by τ are moved by a single cycle appearing in the decomposition of σ.

Since $\sigma(V_1) = V_1$ and $\tau(V_1) = V_1$, we obtain a homomorphism ρ of $G = \langle \sigma, \tau \rangle$ into $\mathrm{Sym}(V_1)$ defined by letting $\rho(\eta)$ be the restriction to V_1 of $\eta \in G$. Thus $\rho(\sigma) = \xi_1$ and $\rho(\tau) = \tau$. The group $\rho(G) = \langle \xi_1, \tau \rangle$ is determined by Theorem 3 since ξ_1 is a cycle on V_1 and τ is a transposition. The kernel of ρ is the set of elements in G that leave fixed each element of V_1.

We will describe the kernel of ρ precisely but first we examine a potentially larger group containing G.

Let $\gamma = \xi_1^{-1}\sigma$ so that

$$\sigma = \xi_1\xi_2 \cdots \xi_r = \xi_1\gamma = \gamma\xi_1 .$$

Of course ξ_1 need not be in G so γ need not be in G. Let $\mathscr{G}$ be the group generated by σ, τ, and γ. Then we also have $\mathscr{G} = \langle \xi_1, \tau, \gamma \rangle$. The subgroup $\langle \xi_1, \tau \rangle$ of $\mathscr{G}$ operates on V_1 while fixing each point in its complement and $\langle \gamma \rangle$ operates on the complement of V_1 while fixing each point of V_1. It follows that the group $\mathscr{G}$ is the direct product

$$\mathscr{G} = \langle \xi_1, \tau \rangle \times \langle \gamma \rangle . \qquad (*)$$

The subgroup of $\mathscr{G}$ fixing V_1 is $\langle \gamma \rangle$ and so the kernel of $\rho : G \to \langle \xi_1, \tau \rangle$ is the cyclic group $G \cap \langle \gamma \rangle$.

The subgroup S of $\langle \xi_1, \tau \rangle$ generated by all the conjugates of τ is actually a subgroup of G. To see this we note that any element η of G can be expressed as

$$\eta = \rho(\eta)\gamma^i \quad \text{for some integer} \quad i .$$

Thus

$$\eta\tau\eta^{-1} = \rho(\eta)\gamma^i\tau\gamma^{-i}\rho(\eta)^{-1} = \rho(\eta)\tau\rho(\eta)^{-1} .$$

Since ρ maps G onto $\langle \xi_1, \tau \rangle$ it follows that every conjugate of τ in $\langle \xi_1, \tau \rangle$ is also conjugate of τ in G and conversely. The subgroup generated by all these conjugates, denoted as S in Theorem 3, is contained in G and in the first factor of $\mathscr{G}$ in (*).

We will factor out the normal subgroup S from both G and $\mathscr{G}$. Since $\tau \in S$ it follows that

$$\frac{\mathscr{G}}{S} \cong \langle \bar{\xi}_1 \rangle \times \langle \bar{\gamma} \rangle ,$$

$$\frac{G}{S} \cong \langle \bar{\sigma} \rangle = \langle \bar{\xi}_1\bar{\gamma} \rangle ,$$

where $\bar{\eta}$ is the coset ηS. This factor will be used in two ways: We will determine the index of S in G and thereby determine the order of G and we will also determine the smallest power of γ that lies in G thereby finding the kernel of ρ.

We are dealing with a two-generator abelian group $\mathscr{G}/S$ and the subgroup G/S generated by the product of the two generators. The first generator $\bar{\xi}_1$ has order t, the number of connected components of the graph $\Gamma(\xi_1, \tau)$. Let g denote the order of γ. Note that g is also the order of $\bar{\gamma}$ because $S \cap \langle \gamma \rangle = e$. Then the order of $\bar{\sigma} = \bar{\xi}_1\bar{\gamma}$ is the least common multiple of t and g, denoted as $[t, g]$. Thus the order of G is the order of S times $[t, g]$. The order of $\langle \xi_1, \tau \rangle$ is the order of S times t (as we known from Theorem 3) and ρ maps G onto this group. Hence the kernel of ρ has order

$$|\ker \rho| = \frac{|S|\,[t, g]}{|S|\,t} = \frac{[t, g]}{t} = \frac{g}{(t, g)},$$

where (t, g) is the greatest common divisor of t and g. Since the order of γ^t is $g/(t, g)$ it follows that γ^t generates the kernel of ρ; we have $G \cap \langle \gamma \rangle = \langle \gamma^t \rangle$.

We summarize this case in a theorem.

THEOREM 5. *Suppose* $\sigma = \xi_1\xi_2 \cdots \xi_r$ *is the cycle decomposition of* σ *and* $\tau = (a, b)$ *is a transposition with both* a *and* b *moved by the cycle* ξ_1 *appearing in* σ. *Let* $G = \langle \sigma, \tau \rangle$. *Let* $\gamma = \xi_1^{-1}\sigma$ *and let* n *be the order of* ξ_1, g *the order of* γ *and* t *the number of connected components of the graph* $\Gamma(\langle \xi_1, \tau \rangle, \tau)$ *and* $k = n/t$. *Then the subgroup* S *of* G *generated by all the G-conjugates of* τ *is isomorphic to the direct product of* t *copies of* Sym(k). *The quotient group* G/S *is cyclic with order* $[t, g]$, *the least common multiple of* t *and* g. *The order of* G *is* $(k!)^t[t, g]$. *The homomorphism* $\rho: G \to \langle \xi_1, \tau \rangle$ *defined by restricting the action of* G *to the set of symbols moved by* ξ_1 *has kernel* $\langle \gamma^t \rangle$.

Example 3. This example illustrates the ideas used in the proof of Theorem 5. Let $\sigma = (1, 2, 3, 4, 5, 6)(7, 8, 9)$ and $\tau = (1, 3)$. Then $\xi_1 = (1, 2, 3, 4, 5, 6)$ and $\gamma = (7, 8, 9)$ in the notation of Theorem 5. We first describe the group $\langle \xi_1, \tau \rangle$ using Theorem 3 and the graph $\Gamma = \Gamma(\langle \xi_1, \tau \rangle, \tau)$. The lowest power of ξ_1 that has the same effect as τ on 1 is ξ_1^2. Thus the number of components of Γ is $t = gcd(6, 2) = 2$. Thus the components of Γ have vertex sets $\{1, 3, 5\}$ and $\{2, 4, 6\}$ as we find by applying powers of ξ_1 to $\{1, 3\}$. Thus the subgroup generated by the G-conjugates of r is $S = S_1 \times S_2$ with each $S_i \cong \mathrm{Sym}(3)$.

The group $G = \langle \sigma, \tau \rangle$ admits a homomorphism ρ onto $\langle \xi_1, \tau \rangle$ defined by restriction of elements of G to the action induced on $\{1, 2, 3, 4, 5, 6\}$, the set moved by ξ_1. The kernel of ρ is the subgroup of G fixing the symbols 1, 2, 3, 4, 5, 6. The kernel was shown to be $G \cap \langle \gamma \rangle = \langle \gamma^t \rangle$. Since $t = 2$ and $\gamma = (7, 8, 9)$ has order 3, it follows that the kernel of ρ is the group $\langle \gamma \rangle$ of order 3. The group G must also contains $\xi_1 = \gamma^{-1}\sigma$ and so we have the decomposition

$$\begin{aligned} G &= \langle \sigma, \tau \rangle = \langle (1, 2, 3, 4, 5, 6)(7, 8, 9), (1, 3) \rangle \\ &= \langle \xi_1, \tau \rangle \times \langle \gamma \rangle = \langle (1, 2, 3, 4, 5, 6), (1, 3) \rangle \times \langle (7, 8, 9) \rangle . \end{aligned}$$

The order of G is $(3!) \cdot 2 \cdot 3 = 6^3$.

If this example is changed by letting $\sigma = (1, 2, 3, 4, 5, 6)(7, 8)$, so that $\gamma = (7, 8)$, but keeping the same τ then t is unchanged and so the kernel of ρ is $\langle \gamma^2 \rangle = e$. Thus $\rho\colon G \to \langle \xi_1, \tau \rangle$ is an isomorphism. The order of G is $(3!)^2 \cdot 2$.

The two cases covered by Theorems 3 and 5 take care of the difficult cases. All the remaining cases can be handled quickly.

Third Case. $\tau = (1, 2)$ and $\sigma(1) = 1$ and $\sigma(2) = 2$; *i.e.* σ fixes the two symbols moved by τ. Then

$$G = \langle \sigma, \tau \rangle = \langle \sigma \rangle \times \langle \tau \rangle$$

is the direct product of two cyclic groups.

Fourth Case. $\tau = (1, 2)$ and $\sigma = (1, a_2, \cdots, a_r)\,(2, b_2, \cdots, b_s)\gamma$ where $r \geqslant 1, s \geqslant 1$; *i.e.* σ moves at least one of the symbols moved by τ and if it moves both, they do not appear in the same cycle of σ. If $r = 1$ then $\sigma(1) = 1$; similarly for $s = 1$. If $r = s = 1$ then we are in the third case so we may assume either r or s is greater than 1. It is assumed that this is the cycle decomposition of σ and that γ is the product of the disjoint cycles not moving 1 or 2. Then we let σ_1 be the element

$$\begin{aligned} \sigma_1 = \sigma\tau &= (1, a_2, \cdots, a_r)(2, b_2, \cdots, b_s)\gamma(1, 2) \\ &= (1, b_2, \cdots, b_s, 2, a_2, \cdots, a_r)\gamma . \end{aligned}$$

Since the group generated by σ and τ is the same as the group generated by σ_1 and τ, we may replace σ by σ_1. We are back in the first case now because both 1 and 2 are moved by the same cycle appearing in the generator σ_1.

We may collect the results as follows.

SUMMARY. Let $G = \langle \sigma, \tau \rangle$ with $\sigma, \tau \in \mathrm{Sym}(n)$ and τ a transposition.

1. If σ is an n-cycle, the G is described in Theorem 3.
2. If σ is a product of disjoint cycles, one of which moves both the symbols moved by τ, then G is described in Theorem 5.
3. If σ fixes both symbols moved by τ then $G = \langle \sigma \rangle \times \langle \tau \rangle$ is an abelian group.
4. If σ moves one, but not both of, the symbols moved by τ or if σ moves both symbols moved by τ but not in the same cycle then σ may be replaced by $\sigma_1 = \tau\sigma$ and then $G = \langle \sigma_1, \tau \rangle$ and G is described as in case 1 or 2.

REFERENCES

[1] JACOBSON, N. *Basic Algebra.* W. H. Freeman and Co., San Francisco, 1974.
[2] JANUSZ, G. and J. ROTMAN. Outer Automorphisms of S_6. *Amer Math. Monthly 89, No. 6* (1982), 407-410.
[3] JORDAN, C. *Traité des substitutions et des Equations Algébriques.* 1870 (Note C).
[4] ROTMAN, J. *Theory of Groups, 3rd Ed.* Allyn & Bacon, Inc. Boston, 1984.

(Reçu le 7 mai 1991)

Gerald J. Janusz

University of Illinois, Urbana, IL
Mathematical Reviews, Ann Arbor, MI