

Transitive Subgroups of S_5

Patrick J. Morandi

Mathematics 581

What are the possible Galois groups of a separable, irreducible polynomial of degree 5? By a homework problem in section 5, any such group is isomorphic to a transitive subgroup of S_5 , whose order is a multiple of 5. The only divisors of $|S_5| = 120$ which are multiples of 5 are 5, 10, 15, 20, 30, 40, 60, and 120. Of these orders, which groups occur? We determine this now.

First, we see that transitivity is vacuous.

Proposition 1 *Let G be a subgroup of S_5 with $|G|$ a multiple of 5. Then G is a transitive subgroup of S_5 .*

Proof. By Cauchy's theorem, G contains an element of order 5. The only elements of S_5 of order 5 are the 5-cycles. However, if σ is a 5-cycle, then for each $i, j \in \{1, 2, 3, 4, 5\}$, there is a power of σ which sends i to j . Therefore G is transitive. ■

There are some restrictions on elements of S_5 . If a permutation is written as a product of disjoint cycles, then its order is the least common multiple of the lengths of the cycles. Therefore, the only possible orders are 1, 2, 3, 4, 5, and 6. This will help us eliminate some groups from being subgroups of S_5 . For a piece of notation, let C_n be a cyclic group of order n .

The first case to consider is a subgroup of order 5. Any group of order 5 is cyclic, so is isomorphic to C_5 . The subgroups of S_5 of order 5 are the subgroups generated by a 5-cycle.

Next we consider groups of order 10. The only abelian group of order 10 is $C_5 \times C_2 \cong C_{10}$. However, there is no element of order 10 in S_5 , so C_{10} is not a subgroup of S_5 . The group D_5 , the symmetries of a regular pentagon, can be viewed as a subgroup of S_5 by viewing D_5 as a certain collection of permutations of its vertices. Generators of D_5 consist of a rotation by an angle of $2\pi/5$, and a flip, holding one vertex fixed. To get a concrete representation of D_5 as a subgroup of S_5 , we label the vertices from 1 to 5 in order counterclockwise. The rotation by $2\pi/5$ is then the cycle (12345) , and the flip holding vertex 2 fixed is $(13)(45)$. The group $\langle (12345), (13)(45) \rangle$ is then a subgroup of S_5 isomorphic to D_5 . A group theory

exercise using Sylow theory (and semidirect products) shows that there is a unique up to isomorphism nonabelian group of order pq if $p < q$ are primes and p divides $q - 1$. Thus, D_5 is the unique nonabelian group of order 10. We have thus accounted for all subgroups, up to isomorphism, of S_5 of order 5 or 10.

We next rule out subgroups of order 30 or 40. Suppose there is a subgroup H of order either 30 or 40. Then $|S_5 : H| = 3$ or $|S_5 : H| = 4$. To see this cannot happen, we use some group theory.

Proposition 2 *If G is a finite group and H a nontrivial subgroup, such that $|G|$ does not divide $|G : H|!$, then H contains a nontrivial normal subgroup of G .*

Proof. This is Theorem 2.4.2 in Walker's book [2], or Lemma 2.9.1 in Herstein's book [1]. The idea is that G acts on the set of left cosets G/H of H in G , which induces a homomorphism $G \rightarrow S_n$, where $n = |G : H|$. Moreover, the kernel of this homomorphism is contained in H . If $|G|$ does not divide $n!$, then the kernel is a nontrivial normal subgroup of G contained in H . ■

Proposition 3 *The alternating group A_5 is simple. Therefore, the only nontrivial normal subgroup of S_5 is A_5 .*

Proof. This is Theorem 2.5.7 and Corollary 2.5.8 of [2]. ■

From these group theory facts, we can now see there is no subgroup of S_5 of order 30 or 40. If there was a subgroup H of order 30 or 40, then $|S_5|$ would not divide $|S_5 : H|!$, hence H would contain a nontrivial normal subgroup of S_5 , which cannot happen since A_5 is the only nontrivial normal subgroup of S_5 . Thus, there is no subgroup of S_5 of order 30 or 40.

This leaves us to consider groups of order 15 or 20. For order 15, by the Sylow theorems any group of order 15 has a normal subgroup P of order 5 and a normal subgroup Q of order 3. Since $P \cap Q = \langle e \rangle$, this forces the group to be the direct product $P \times Q$, hence a cyclic group of order 15. As noted before, there is no element of order greater than 6, so there is no subgroup of S_5 of order 15.

For subgroups of order 60 or 120, clearly S_5 is the only subgroup of S_5 of order 120. Also, A_5 is the only subgroup of order 60, which we can see by using the two group theory results above together with the group theory exercise that says any subgroup of index 2 is normal in the larger group.

Finally, we consider groups of order 20. This is the hardest case. Suppose G is a subgroup of S_5 with $|G| = 20$. By the Sylow theorems, there is a normal subgroup N of G of order 5. Also, there is a subgroup H of order 4. This makes G the semidirect product of N and H . What we use to describe G are the essential ideas of semidirect products. One can check

that the map $\varphi : H \rightarrow \text{Aut}(N)$ given by $\varphi(h) : n \rightarrow hnh^{-1}$ is a group homomorphism. Moreover, $NH = \{nh : n \in N, h \in H\} = G$. If $h \in \ker \varphi$ and if $N = \langle a \rangle$, then $hah^{-1} = a$, so $ha = ah$. A short calculation shows that ha has order 10, which is impossible. Therefore, φ is 1-1. However, $\text{Aut}(N) \cong C_4$ (see Example 2.8.1 of [1] or Theorem 2.3.16 of [2]), which forces $H \cong C_4$ since $|H| = 4$. By a closer analysis of semidirect products, one can show that there is a unique up to isomorphism group G such that (i) $|G| = 20$, and (ii) G has no element of order 10. To see that this group occurs as a subgroup of S_5 , we note that $x^5 - 2$ is a separable, irreducible polynomial over \mathbb{Q} , so if $K = \mathbb{Q}(\sqrt[5]{2}, \exp(2\pi i/5))$ is its splitting field, then $\text{Gal}(K/\mathbb{Q})$ is isomorphic to a subgroup of S_5 , and this group is a nonabelian group of order 20. To get a concrete representation of this group, we need elements $a, b \in S_5$ with a of order 5, b of order 4, and $bab^{-1} = a^2$. This last equation comes from the mapping φ above. A generator of $\text{Aut}(C_5)$ is the automorphism σ defined by $\sigma(u) = u^2$ for any $u \in C_4$. We can choose a to be any 5-cycle, so pick $a = (12345)$. To find b so that $b(12345)b^{-1} = (12345)^2 = (13524)$, by the calculation at the bottom of page 88 in [1], we can choose b to send the i -th element listed in (12345) to the i -th element listed in (13524) . That is, $b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix} = (2354)$.

The isomorphism classes of subgroups of S_5 of order a multiple of 5 are listed in the following table, along with a concrete representation as a subgroup.

Group	Representation
C_5	$\langle (12345) \rangle$
D_5	$\langle (12345), (13)(45) \rangle$
$C_5 \rtimes C_4$	$\langle (12345), (2354) \rangle$
A_5	
S_5	

References

- [1] I. N. Herstein, *Topics in Algebra*, John Wiley and Sons, 1975.
- [2] E. Walker, *Introduction to Abstract Algebra*, Random House, 1987.