

The purpose of these notes is to explain an argument used by Galois to describe when equations of prime degree are solvable by radicals. One of the difficulties of reading Galois is that what he calls a group does not seem to be the same as what we call a group. He seems to pass between groups and cosets of groups rather freely to the point that it is not always clear which one he means. Also, of course, he views everything as a subgroup of permutation groups. On the other hand, if you can read French even a little bit, it is well worth the trouble to try to read Galois. One benefit is that, since the theory had not yet been developed when Galois wrote, every argument is as simple and direct as possible with a minimum of abstraction.

The following is a case in point.

Theorem 1. (Galois). *Let p be a prime number. Let S_p denote the symmetric group on p letters and let C_p denote the cyclic group generated by any cycle γ of length p in S_p . Then the largest solvable subgroup of S_p containing C_p is the normalizer N_p of C_p in S_p .*

In fact, as we will see below, the fact that S_p is not solvable for $p > 3$ is a corollary of the theorem. We begin with a result from Proposition VII of Galois' memoir. (In the memoir, the word "Proposition" seems to denote a section in the manuscript.)

Lemma 2. *The group N_p has order $p(p-1)$. It is isomorphic to the subgroup L_p of functions $x \mapsto ax + b$ from \mathbf{F}_p to itself where $a \in \mathbf{F}_p^\times$ and $b \in \mathbf{F}_p$. (Here \mathbf{F}_p denotes the field with p elements. The elements of L_p are called affine transformations.)*

Proof. Without loss of generality, we can assume that the generator γ of C_p is the cycle $(12 \cdots p)$. We can think of S_p as the group of all one-to-one maps from \mathbf{F}_p to itself. Then γ is the function $x \mapsto x + 1$. Suppose $f \in S_p$ normalizes C_p . Then there exists $a \in (\mathbf{Z}/p)^\times$ such that $f\gamma f^{-1} = \gamma^a$. Thus, for all $x \in \mathbf{Z}$, $f\gamma^x f^{-1} = \gamma^{ax}$. Thus $f\gamma^x = \gamma^{ax}f$. Therefore the equation $f(i+x) = f(i) + ax$ holds for all i, x . Now take $i = 0$ and get that, for all x , $f(x) = ax + f(0)$. This shows that $N_p \subset L_p$. It is easy to see (by explicit computation) that every element of L_p normalizes C_p . Therefore, since L_p clearly has $(p-1)p$ elements, the lemma follows. Q.E.D.

Recall that we say a subgroup $H \leq K$ is *characteristic* if any automorphism of K preserves H . For example, it is easy to see that C_p is characteristic in N_p because C_p is the unique subgroup of order p in N_p . This follows directly from Sylow because C_p is normal in N_p and $|N_p| = (p-1)p$. However, it could also be proved by direct computation.

Lemma 3. *Suppose $H \leq K \triangleleft G$ are groups, and suppose that H is a characteristic subgroup of K . Then H is normal in G .*

Proof. If K is normal in G then G acts on K by inner automorphisms. These must preserve H . Thus H must be normal in G . Q.E.D.

Let us call a subgroup $G \leq S_p$ *transitive* if G acts transitively on $\{1, \dots, p\}$. Note that any subgroup of S_p isomorphic to C_p is transitive. So any subgroup containing an element of order p is transitive. Conversely, since p divides the order of any transitive subgroup, any transitive subgroup contains an element of order p .

The next lemma is a reformulation of Galois' Proposition VI in page 429 of the *Memoire* (which corresponds to page 53 of the text linked on the class web site).

Lemma 4. *Let G be a transitive subgroup of S_p for p prime and let H be a non-trivial normal subgroup of G . Then H is transitive.*

Proof. Since G acts transitively on $\{1, \dots, p\}$, the stabilizers $G_i := \{g \in G \mid gi = i\}$ are all conjugate in G . Therefore, since H is normal in G , the stabilizers $H_i = G_i \cap H$ are all conjugate in G as well. It follows that the orbits of H all have the same number of elements. Therefore, since p is prime, this number must be either 1 or p . Q.E.D.

Proof of Theorem 1. Let $f_{a,b}$ denote the element of N_p given by $x \mapsto ax + b$. Then $f_{a,b}f_{c,d}(x) = a(cx + d) + b = ac + (ad + b)$. Thus $f_{a,b}f_{c,d} = f_{ac,ad+b}$. It follows that the map $N_p \rightarrow \mathbf{F}_p^\times$ given by $f_{a,b} \mapsto a$ is a (surjective) group homomorphism with kernel isomorphic to C_p . Therefore we have an exact sequence

$$1 \rightarrow C_p \rightarrow N_p \rightarrow \mathbf{F}_p^\times \rightarrow 1.$$

Hence, since C_p and \mathbf{F}_p^\times are abelian, N_p is solvable.

Now, suppose there is a solvable subgroup of S_p containing a cyclic subgroup C_p of order p in S_p which is not contained in the normalizer N_p of C_p . Let G denote one which has a composition series

$$\{1\} \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_r$$

of minimal length. Clearly, $r > 1$ since, if $r = 1$, we must have $G_1 = C_p$. Therefore, by Lemma 4, G_{r-1} is transitive. Therefore G_{r-1} contains an element γ' of order p . It follows, from the minimality of r , that G_{r-1} is contained in the normalizer N'_p of the subgroup C'_p of S_p generated by γ' . Now, C'_p is characteristic in G_{r-1} because it is the unique subgroup of order p . Therefore, by Lemma 3, $G_r \leq N'_p$. But this implies that $C_p = C'_p$ since $C_p \leq G_r$ and C'_p is the unique subgroup of order p in N'_p .

Corollary 5. *The group S_p is not solvable for $p > 3$.*

Proof. Since the order of N_p is $(p-1)p$, N_p is smaller than G for $p > 3$.

Remark. The theorem may be used to solve one of the problems on the homework concerning Galois groups of degree 5 equations.

Galois draws the following consequence from Theorem 1.

Theorem 6. (Galois) *Let f be an irreducible polynomial of prime degree p over a field F of characteristic 0. Let E be the splitting field of f and let $\alpha_1, \dots, \alpha_p$ be the roots of f in E . Then the following are equivalent: (i) f is solvable, (ii) there exists $1 \leq i < j \leq p$ such that $E = F[\alpha_i, \alpha_j]$, (iii) for any $1 \leq i < j \leq p$, we have $E = F[\alpha_i, \alpha_j]$.*

Proof. Set $G = \text{Gal}(E/F)$. Suppose $E = F[\alpha_1, \alpha_2]$. Then $|G| \leq p(p-1)$. It follows that the p -Sylow in G is normal. Thus G is contained in a group isomorphic to N_p and is thus solvable. Thus (ii) \Rightarrow (i).

Suppose conversely that E/F is solvable. Then, by Theorem 1, G is contained in N_p . We can view G then as a subgroup of L_p so that the action of G on the roots is given by $f_{a,b}\alpha_x = \alpha_{ax+b}$ (where the indexes are read modulo p). Suppose $1 \leq i < j \leq p$. Then $f_{a,b}\alpha_i = \alpha_i, f_{a,b}\alpha_j = \alpha_j \Rightarrow$

$$\begin{aligned} ai + b &= i \\ aj + b &= j. \end{aligned}$$

Therefore $(a-1)(i-j) = 0 \Rightarrow a = 1 \Rightarrow b = 0$. It follows that $\text{Gal}(E/F[\alpha_i, \alpha_j]) = \{1\}$. Thus $E = F[\alpha_i, \alpha_j]$. Since i, j were arbitrary it follows that (i) \Rightarrow (iii).

It is obvious that (iii) \Rightarrow (ii).

Q.E.D.

Acknowledgment. I thank Hannah Cairns for email correspondence which helped me understand Galois' proof of Lemma 4.