Galois' Theorem

The following is attributed by Jacobson to Galois in *Basic Algebra I*. For notational purposes, p will always be a prime, and F a field of characteristic 0.

Theorem 1. *Let $f(x) \in F[x]$ be irreducible of degree p. Suppose M is the splitting field of f over F and G is the Galois group of M/F. Then G is solvable if and only if $M = F(r_1, r_2)$ for any two roots r_1 and r_2 of f.*

We remark that the conditions of Theorem 1 are well-known to be the conditions for f to be solvable by radicals.

Theorem 1 will follow from a group-theoretic equivalent. We pave the way for that. Suppose H is the subgroup of G fixing r_1 and r_2, where r_1 and r_2 are distinct roots. Then $F(r_1, r_2) = M$ if and only if $H = (1)$. Thus we are asked to show that an automorphism fixing more than one root must be the identity. This makes Theorem 1 equivalent to the following:

Theorem 2. *Suppose G is a transitive group of degree p. Then the following are equivalent*

(1) G is solvable
(2) For every $\sigma \neq 1$ in G, σ has at most one fixed point
(3) G has a normal subgroup T of order p such that $T = C_G(T)$

Moreover, if these conditions apply, then $G = MT$ where M is a cyclic group of order dividing $p - 1$

The remarks above should be enough to convince you that Theorems 1 and 2 are equivalent (using item (2)).

The following is useful for the proof of Theorem 2. It is a well-known counting principle that often shows up on qualifying exams:

Lemma 1. *Suppose G is a finite group acting on a set S. For $g \in G$, let $C(g) =$ the number of fixed points of g in S. Then:*

$$\#\text{ of orbits of } G = \sum_{\sigma \in G} \frac{C(g)}{|G|}$$

We procede to the proof of Theorem 2 in sections.

1) $\Rightarrow$ 3):

Let T be a minimal normal subgroup of G. The normality assures that all orbits of T have the same size, and this size divides the number of elements p (check). Thus, each normal subgroup has orbit size 1 or p. Since all orbits of size 1 would make T trivial, we conclude that T is transitive on the p elements. We wish to show T has order p. Let G' be the commutator subgroup of G. If $G' = \langle 1 \rangle$, then G is abelian, and the elements of order p are a normal subgroup. We may then suppose that $\langle 1 \rangle \neq G' < G$, as G is solvable. As G' is a normal subgroup, we must have that p divides $|G'|$ by the argument above, and then by induction G' has a normal subgroup N of order p. Now N is a normal subgroup of a characteristic subgroup, so $N = T$ is normal in G. We have settled the issue that G has a normal subgroup of order p.

It remains to show that $T = C_G(T)$. Let $T = \langle t \rangle$, and suppose $\sigma t = t\sigma$. Then $H = \langle t, \sigma \rangle$ is an abelian subgroup which acts transitively, as all elements in T are p-cycles. Now $H = T \times U$ where $|U|$ is prime to p. By the argument above, $U = \langle 1 \rangle$, and so $H = T \Rightarrow \sigma \in T$.

3) $\Rightarrow$ 2):

Suppose $1 \neq \sigma \in G$, and we may suppose $\sigma(1) = 1$ where $T = \langle t \rangle$ and $t = (123 \ldots p)$. We must show σ has no other fixed points. If σ commutes with t, then $\sigma \in T$ and has no fixed points. Thus we may suppose

a) $$\sigma t \sigma^{-1} = t^i, \quad i \neq 1 \pmod{p}$$

All calculations from now on will be done modulo p. We will also be sloppy about the distinction between the numeral 1 and the 1 in G. Evaluating both sides of a) at 1 gives:

b) $$\sigma(2) = t^i(1) = i + 1$$

Note that $\sigma(2) \neq 2$ since $i \neq 1$. Now evaluate both sides of b) at $\sigma(2)$ to get:

$$\sigma(3) = t^i(i+1) = 2i + 1$$

Again, $\sigma(3) \neq 3$ as $i \neq 1$. Proceeding inductively, we get

$$\sigma(j) = (j-1)i + 1 \quad \text{for } 1 < j \leq p$$

and so $\sigma(k) = k$ if and only if $k = 1$.

2) $\Rightarrow$ 3):

Let $T = \langle t \rangle$ be a subgroup of G of order p. We use Lemma 1 (noting there is one orbit as G is transitive) in the form:

c) $$|G| = \sum_{g \in G} C(g)$$

The identity in T has p fixed points, and the $p-1$ non-identity elements in T have none. Thus, the contribution of T to the right side of c) is p. The other $|G| - p$ elements in $G - T$ can contribute at most one fixed point, and each must contribute exactly one to make sure the right side of c) is not smaller than $|G|$. It follows that the non-identity elements of T are the only ones with no fixed points, and all other non-identity elements in G have one fixed point. This shows that T is normal in G.

Suppose now that $\sigma t = t\sigma$. If σ has no fixed points, then $\sigma \in T$, so we may suppose $\sigma(1) = 1$. Then $\sigma t(1) = t\sigma(1) = t(1)$, and so σ fixes both 1 and $t(1)$, which says $\sigma = 1$.

Finally, suppose G satisfies 2) and 3). We fix a generator t of T. Let C be the group of non-0 elements modulo p. Consider the map ϕ from G to C given by:

$$\phi(g) = i \quad \text{if } gtg^{-1} = t^i$$

This map is a homomorphism since $\phi(g) = i$ and $\phi(h) = j$ implies

$$ghth^{-1}g^{-1} = gt^j g^{-1} = (gtg^{-1})^j = (t^i)^j = t^{ij}$$

The kernel of ϕ is $C_G(T) = T$, and so G/T is isomorphic to a subgroup of C, which is a cyclic group of order $p-1$. This implies that

$$1 \longrightarrow T \longrightarrow G \longrightarrow G/T \longrightarrow 1$$

is split, and the remaining statements of Theorem 2 follow.

Don't even ask me how Galois did this ...