

Handout 25: Galois theory, part VII: (un)solvability

Theorem (5.38). For all $n \geq 5$, a general quintic polynomial f is not solvable by radicals.

Remember we say that $f(x) \in k[x]$ is solvable by radicals if there is some radical extension K of k containing a splitting field E for f over k .

Here are the two crucial ingredients in the proof of Theorem 5.38:

- (1) **Definition.** The group G is called *solvable* if there exists a descending normal series

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_t = \{1_G\}$$

in which the *factor groups* G_{i-1}/G_i are all finite cyclic groups of prime order p_i for $i = 1, \dots, t$.

- (2) **Theorem (5.34/5.37/Exercise 5.28).** If $f \in k[x]$ is solvable by radicals and has splitting field E over k , then $\text{Gal}(E/k)$ is a solvable group.

We'll skim over the proof of this last result. It (at least with appropriate simplifying assumptions) follows from our recent result giving us a descending normal series of Galois groups arising from the intermediate extensions in a radical tower.

Your textbook gives a technical proof of Theorem 5.38 in full generality on page 468, but I find that a more specific example is more understandable and more illuminating.

Example. Let $k = \mathbb{Q}$ and let $f(x) = x^5 - px + p \in k[x]$ where $p \geq 13$ is prime, and let E be a splitting field for f over k , contained in \mathbb{C} . We will show that $\text{Gal}(E/k) \cong S_5$, which is not solvable.

- (1) First of all, we note that A_5 is a simple group (recall this means that it has no nontrivial normal subgroups); in fact every A_n , $n \geq 5$, is simple. This implies that the only chain of normal subgroups in S_5 is

$$S_5 \supseteq A_5 \supseteq \{1\}.$$

Since the factors in this chain are not cyclic groups at all (let alone of prime order), S_5 cannot be solvable. Therefore we're done if we show that $\text{Gal}(E/k) \cong S_5$ is true.

- (2) Next, let's count the real roots of f , the old fashioned way: How many local extrema does f have, and where?

- (3) It's not too much work to show the positive extremum, call it y , is a minimum and the negative one is a maximum.

- (4) Let's see if we can estimate $f(y)$, and explain how this tells us the number of real roots f has:
- (5) We know already that $\text{Gal}(E/k)$ is isomorphic to a subgroup of S_5 . Since we now know that there are three real roots, there are two complex roots, appearing as a conjugate pair. Therefore the restriction of complex conjugation to E gives an automorphism of E that permutes these two roots. That is, $\text{Gal}(E/k)$ contains a transposition, and without loss we can write this transposition as $(1\ 2)$.
- (6) We know that for any of the root z of f , E is an extension of $k(z)$, which is an extension of k . Why does this imply 5 divides $|\text{Gal}(E/k)|$?
- (7) It turns out that the only elements of order 5 in S_5 are cycles of order 5, and since $\text{Gal}(E/k)$ must contain an element of order 5, we've got a cycle σ of order 5 in $\text{Gal}(E/k)$. Without loss, let's denote it by $\sigma = (1\ 2\ 3\ 4\ 5)$.
- (8) Compute $\sigma(1\ 2)\sigma^{-1}$ and $(1\ 2)\sigma(1\ 2)\sigma^{-1}(1\ 2)$.
- (9) Can you see how this (suitably elaborated) implies that $\text{Gal}(E/k)$ contains *all* of S_5 ?