Lecture 35: The Quintic Formula, Cont.

Monday, November 30, 2020

Last time, we proved that every radical extension of characteristic 0 field is contained in a solvable extension. We now want to use this to prove that there are equations that don't have a radical solution.

Take equations of quadratic form, $x^2 + bx + c = 0$. We know that the roots are given by the quadratic equation:

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

Theorem 0.0.1. *There exists a degree-5 equation with $\mathbb{Z}$-coefficients whose roots are not in a radical extension.*

Lemma 0.0.2. *If $p \in \mathbb{Q}[x]$ all of prime degree and all but 2 of whose roots are real, then the Galois group of p in $\mathbb{Q}$ is S_n where $n = \deg p$.*

Proof. Suppose G is the Galois group of p. We can think of G as the group which permutes the roots of p. $G \leq \mathrm{Sym}(\text{roots of p})$. We will call the roots of p R. G acts transitively on R, i.e. R is the orbit of G.

The reason for this is the following. K is a splitting field of p such that $G = \mathrm{Gal}(K/\mathbb{Q})$. If $r \in R$, $f \equiv \prod_{r' \in Gr}(x - r')$. f is fixed by G, such that $\tau f = \prod_{r' \in Gr}(x - \tau r')$, so $f \in \mathrm{Fix}(G)[x] = \mathbb{Q}[x]$.

Because G acts transitively on R, $R = \frac{|G|}{|G_r|}$ where G_r is the stabilizer of some $r \in R$ (from very early in this class). We assumed that $|R| = n$ is prime, so $n \mid |G|$.

By Cayley's theorem, there exists an element $g \in G$ of order n, so g is an n-cycle on R. Indeed, if g is a product of an a_1-cycle, a_2-cycle, a_3-cycle, etc., then the order of $g = \mathrm{lcm}(a_1, a_2, a_3, \cdots)$.

Now we will use the assumption that all but two roots are real. Since complex conjugation is an automorphism of $\mathbb{C}$ and hence of $K \subseteq \mathbb{C}$, it gives us an element $g' \in G$ which is a transposition on R. We have shown that the Galois group contains two elements, an n-cycle on the roots and this transposition:

$$S_n = \langle (12 \cdots n), (ij) \rangle$$

□

Now for the proof of the original theorem:

Proof. Take $p = x^5 - 4x + 2$. This is irreducible in $\mathbb{Q}$ using the Eisenstein theorem for prime 2. The derivative is $p' = 5x^4 - 4$, so the roots of p' are $\pm(4/5)^{1/4}$ and those are simple. □

Theorem 0.0.3. *If K/F is a degree n extension and $\mathrm{char}(F) \nmid n$ and F contains all nth roots and K/F is cyclic, then $K = F(\sqrt[n]{a})$ for $a \in F$.*

If we have a solvable extension K/K_0 with Galois group G, then $\frac{G_{m+1}}{G_m}$ are cyclic. Suppose there is a sequence of extensions K_n between K and K_0. Then if K_0 has enough roots of unity, then the theorem implies that $\frac{K_{i+1}}{K_i}$ are radical.

Definition 0.0.1. The *character* of a field F in a field K is a map $\varphi \colon F^* \to K^*$ that is a homomorphism of abelian groups.

Lemma 0.0.4. *If $\sigma_1, \cdots, \sigma_m$ are distinct characters $F^* \to K^*$, then $\sigma_1, \cdots, \sigma_m$ are linearly independent over K.*

Proof. Induction on m (base case is trivial): Suppose $a_1\sigma_1 + \cdots + a_m\sigma_m = 0$, i.e. $\forall b \in F^*$, $a_1\sigma_1(b) + \cdots + a_m\sigma_m(b) = 0$ (call this equation 1). There must exist some c such that $\sigma_1(c) \neq \sigma_2(c)$. Then, $\forall b$, $a_1\sigma_1(bc) + \cdots = 0$, but this is equal to $a_1\sigma_1(c)\sigma_1(b) + \cdots = 0$ (call this equation 2).

Then $\sigma_1(c)(\text{Eq } 1) - \text{Eq } 2 = a_2(\sigma_1(c) - \sigma_2(c))\sigma_2(b) + \cdots = 0$. The first term in parentheses here is nonzero by definition. □

Corollary 0.0.4.1. *If F/E is Galois and $\sigma_1, \cdots, \sigma_n \in Gal(F/E)$, then $\sigma_1, \cdots, \sigma_n$ are linearly independent over F.*

Now the proof of the theorem:

Proof. Define for $\alpha \in K$ and nth root $w \in F$ the following expression:

$$[\alpha, w] \equiv \alpha + w\sigma(\alpha) + w^2\sigma^2(\alpha) + \cdots + w^{n-1}\sigma^{n-1}(\alpha)$$

where $\text{Gal}(K/F) = \langle\sigma\rangle$. Now examine the action of this generator on the expression:

$$\sigma[\alpha, w] = \sigma(\alpha) + w\sigma^2(\alpha) + \cdots + w^{n-1}\sigma^n(\alpha)$$

Now $\sigma^n(\alpha) = \alpha$ and $w^n = 1$ so we can write

$$\sigma[\alpha, w] = w^{-1}[\alpha, w]$$

Therefore, $\sigma[\alpha, w]^n = [\alpha, w]^n$, so this element is fixed by σ: $[a, w]^n \in \text{Fix}(\langle\sigma\rangle) = \text{Fix}(\text{Gal}) = F$. So we've found some element whose nth power is in F. It now suffices to show that $[F([\alpha, w])\colon F] = n$.

Chose an α such that $[\alpha, w] \neq 0$ using the lemma, because $\text{id} + w\sigma + w^2\sigma^2 + \cdots \neq 0$. If $[F([\alpha, w])\colon F] = m$, this means $[\alpha, w]$ is fixed by σ^m by the Galois correspondence. We know that $\sigma^m[\alpha, w] = w^{-m}[\alpha, w]$, and $w^{-m} = 1 \iff n \mid m$. □