MAT 347
Our last theorem
March 27, 2015

We want to prove that a polynomial has a solvable Galois group if it is solvable by radicals. We already proved the "if" part. Today we prove the "only if" part.

Cyclic Galois group

Let K/F be a normal field extension with characteristic 0. Let $G = \mathrm{Gal}(K/F)$. Assume that G is cyclic of order n. Assume that $X^n - 1$ splits in F. Our first goal is to prove that "K is obtained from F by adding one n-th root." This means we want to find $\alpha \in K$ such that $K = F(\alpha)$ and $\alpha^n \in F$.

1. Let $\theta \in F$ be a primitive n-th root of unity. Let τ be a generator of G. Assume that we find $\alpha \in K$ such that $\alpha \neq 0$ and $\tau(\alpha) = \theta\alpha$. Use Galois theory to prove that this element α is the one we want.

2. Let $\beta \in K$. Find an element $\alpha \in K$ which is a linear combination of

$$\beta, \tau(\beta), \tau^2(\beta), \ldots, \tau^{n-1}(\beta)$$

   which satisfies that $\tau(\alpha) = \theta\alpha$.

3. It remains to prove that we can pick α in the previous question such that $\alpha \neq 0$. The following is a linear-algebra lemma:

   > Let K/F be a field extension. Let $\sigma_1, \ldots, \sigma_m \in \mathrm{Gal}(K/F)$ be *different* elements in the Galois group. Assume there are $t_1, \ldots, t_m \in F$ such that $t_1\sigma_1 + \ldots t_m\sigma_m = 0$. Then $t_1 = \ldots = t_m = 0$.

   Prove this Lemma and use it to complete the proof we were working on.

Solvable Galois group

Let K/F be a normal field extension of characteristic 0. Assume $\mathrm{Gal}(K/F)$ is solvable. Our next goal is to show that there is a field extension R/K such that R/F is radical.

4. Let $|\mathrm{Gal}(K/F)| = m$. Let K_1 be the splitting field of $X^m - 1$ over K. Let $F_1 \subseteq K_1$ be the splitting field of $X^m - 1$ over F. Prove that $\mathrm{Gal}(K_1/F_1)$ is isomorphic to a subgroup of $\mathrm{Gal}(K/F)$.

5. Prove that $\mathrm{Gal}(K_1/F_1)$ is solvable.

6. Prove that $X^n - 1$ splits in F_1 for every n that divides $|\mathrm{Gal}(K_1/F_1)|$.

7. Finally prove that K_1/F_1 is radical.

8. Conclude that a polynomial has solvable Galois group over F iff it is solvable by radicals over F.

Extra: symplifying calculations and Newton's theorem

9. Let $f(X)$ be a polynomial with degree n. Show that there is a number a such that the change of variable $y = x - a$ transforms $f(X)$ into a polynomial $g(Y)$ with degree n and with no term of degree $n-1$.

10. The n elementary symmetric polynomials in the variables $X_1, \ldots, X_n$ are defined as

$$S_k = \sum_{1 \le j_1 < j_2 < \ldots < j_k \le n} \prod_{i=1}^{k} X_{j_i}$$

for $k = 1, \ldots, n$. Write explicitly the elementary symmetric polynomials in the variables α, β, γ.

11. A Theorem by Newton says that if $h(X_1, \ldots, X_n)$ is a symmetric polynomial in n variables, then it can be written in terms of the n elementary symmetric polynomials. As an example, write the following expressions in terms of S_1, S_2, S_3:

- $\alpha^2 + \beta^2 + \gamma^2$,
- $\alpha^3 + \beta^3 + \gamma^3$,
- $\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha + \alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2$.

12. Let $f(X) = X^3 + aX^2 + bX + c$ be a polynomial with roots α, β, γ. Write the coefficients of the polynomial in terms of the roots.

13. In view of the previous problems, interpret the theorem by Newton using Galois theory (and prove it in one line!)