Section X.56. Insolvability of the Quintic

Note. Now is a good time to reread the first set of notes "Why the Hell Am I in This Class?" As we have claimed, there is the quadratic formula to solve all polynomial equations $ax^2+bx+c=0$ (in $\mathbb{C}$, say), there is a cubic equation to solve $ax^3+bx^2+cx+d=0$, and there is a quartic equation to solve $ax^4+bx^3+cx^2+dx+e=0$. However, there is not a general algebraic equation which solves the quintic $ax^5+bx^4+cx^3+dx^2+ex+f=0$. We now have the equipment to establish this "insolvability of the quintic," as well as a way to classify which polynomial equations can be solved algebraically (that is, using a finite sequence of operations of addition [or subtraction], multiplication [or division], and taking of roots [or raising to whole number powers]) in a field F.

Definition 56.1. An extension field K of a field F is an *extension of F by radicals* if there are elements $\alpha_1, \alpha_2, \ldots, \alpha_r \in K$ and positive integers $n_1, n_2, \ldots, n_r$ such that $K = F(\alpha_1, \alpha_2, \ldots, \alpha_r)$, where $\alpha_1^{n_1} \in F$ and $\alpha_i^{n_i} \in F(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})$ for $1 < i \leq r$. A polynomial $f(x) \in F[x]$ is *solvable by radicals over F* if the splitting field E of $f(x)$ over F is contained in an extension of F by radicals.

Note. The idea in this definition is that $F(\alpha_1)$ includes the n_1th root of $\alpha_1^{n_1} \in F$. Then $F(\alpha_1, \alpha_2)$ includes the n_2th root of $\alpha_2^{n_2} \in F$, and so forth. So any element of $F(\alpha_1, \alpha_2, \ldots, \alpha_r)$ can be expressed as a finite number of operations of addition, multiplication, and extraction of roots of elements of F. It is here that extension fields meet up with the idea of algebraic solutions of polynomial equations!!!

Note. For the remainder of this section, we assume that **we are dealing with fields of characteristic 0.**

Note. The outline of this section is:

1. We will show that polynomial $f(x) \in F[x]$ is solvable by radicals over F if and only if its splitting field over F has a solvable Galois group. (We will not actually prove the "if" part.)

2. We will show that there is a subfield F of the real numbers and a polynomial $f(x) \in F[x]$ of degree 5 with a splitting field E over F such that $G(E/F) \cong S_5$.

Notice that S_5 is not solvable, as shown in Example 35.19. Combining (1) (the "only if" part) and (2) will yield the insolvability of the quintic.

Lemma 56.3. Let F be a field of characteristic 0, and let $a \in F$. If K is the splitting field of $x^n - a$ over F, then $G(K/F)$ is a solvable group.

Theorem 56.4. Let F be a field of characteristic zero, and let $F \leq E \leq K \leq \overline{F}$, where E is a normal extension of F and K is an extension of F by radicals. Then $G(E/F)$ is a solvable group.

Note 1. Here's the idea behind Theorem 56.4. We will take $F < \mathbb{R}$, find a polynomial $f(x) \in F[x]$, and let E be the splitting field of $f(x)$. We then assume that K is a field which is an extension of F by radicals that includes all of the zeros of $f(x)$. That is, we assume that $f(x)$ is solvable by radicals and so the zeros are contained in an extension by radicals of F, say K. Then it must be that $G(E/F)$ is solvable. So if $G(E/F)$ is not a solvable group, then $f(x)$ is not solvable by radicals. We will show there is a fifth degree $f(x)$ with $G(E/F) \cong S_5$. Since S_5 is not solvable (by Example 35.19), then $f(x)$ is not solvable by radicals.

Note 2. We are now ready to prove our *final goal*: The Insolvability of the Quintic. As previously mentioned, this means that there exists a fifth degree polynomial which is not solvable by radicals. Of course, this does not mean that *all* fifth degree polynomials are insolvable by radicals. For example, $f(x) = x^5 - x = x(x-1)(x+1)(x^2+1)$ is solvable by radicals—the zeroes are 0, 1, -1, i, $-i$. An explicit example of a fifth degree polynomial that is not solvable by radicals over $\mathbb{Q}$ is (as shown in Exercise 56.8c), $f(x) = 2x^5 - 5x^4 + 5$.

Note. Recall that α is algebraic over F if $f(\alpha) = 0$ for some $f(x) \in F[x]$, and α is transcendental otherwise (Definition 29.3). If α is transcendental over F, then the evaluation homomorphism ϕ_α maps $F[x]$ to an integral domain, denoted $F[\alpha]$. The smallest field containing F and α (a field of quotients of $F[\alpha]$) is denoted $F(\alpha)$. This is explained in more detail in Section 29 (see page 270).

Note. In an introductory analysis class, you will see that the cardinality of the set of algebraic numbers in $\mathbb{R}$ is strictly less than the cardinality of the set of transcendental numbers. The algebraic numbers form a "countable" set and the transcendental numbers form an "uncountable" set. In fact, if α_1 is transcendental, then $\mathbb{Q}(\alpha_1)$ is countable. This implies that there is α_2 transcendental over $\mathbb{Q}(\alpha_1)$, there is α_3 transcendental over $\mathbb{Q}(\alpha_1, \alpha_2)$, etc.

Definition. Let $y_1 \in \mathbb{R}$ be transcendental over $\mathbb{Q}$, $y_2 \in \mathbb{R}$ transcendental over $\mathbb{Q}(y_1)$, $y_3 \in \mathbb{R}$ transcendental over $\mathbb{Q}(y_1, y_2)$, and so forth. Such $y_1, y_2, y_3, \ldots$ are *independent transcendental elements over* $\mathbb{Q}$.

Theorem 56.6. The Final Goal/Abel's Theorem.
Let y_1, y_2, y_3, y_4, y_5 be independent transcendental real numbers over $\mathbb{Q}$. The polynomial

$$f(x) = \prod_{i=1}^{5}(x - y_i)$$

is not solvable by radicals over $F = \mathbb{Q}(s_1, s_2, s_3, s_4, s_5)$ where s_i is the ith elementary symmetric function in y_1, y_2, y_3, y_4, y_5.

Proof. Let $E = \mathbb{Q}(y_1, y_2, y_3, y_4, y_5)$ and let

$$f(x) = \prod_{i=1}^{5}(x - y_i) = x^5 - s_1x^4 + s_2x^3 - s_3x^2 + s_4x - s_5$$

where

$$\begin{aligned} s_1 &= y_1 + y_2 + y_3 + y_4 + y_5 \\ s_2 &= y_1y_2 + y_1y_3 + y_1y_4 + y_1y_5 + y_2y_3 + y_2y_4 + y_2y_5 + y_3y_4 + y_3y_5 + y_4y_5 \end{aligned}$$

$$\begin{aligned} s_3 &= y_1y_2y_3 + y_1y_2y_4 + y_1y_2y_5 + y_1y_3y_4 + y_1y_3y_5 + y_1y_4y_5 \\ &\quad + y_2y_3y_4 + y_2y_3y_5 + y_2y_4y_5 + y_3y_4y_5 \\ s_4 &= y_1y_2y_3y_4 + y_1y_2y_3y_5 + y_1y_2y_4y_5 + y_1y_3y_4y_5 + y_2y_3y_4y_5 \\ s_5 &= y_1y_2y_3y_4y_5, \end{aligned}$$

the elementary symmetric functions in y_1, y_2, y_3, y_4, y_5. Since $s_1, s_2, s_3, s_4, s_5 \in \mathbb{Q}(y_1, y_2, y_3, y_4, y_5) = E$, then $f(x) \in E[x]$. Let $F = \mathbb{Q}(s_1, s_2, s_3, s_4, s_5)$. Then $f(x) \in F[x]$ and $\mathbb{Q} \leq F \leq E$. Now E is the splitting field over F of $f(x)$ (notice that E contains all zeros of $f(x)$). By Theorem 54.2 (with $F = \mathbb{Q}$), the Galois group $G(E/F)$ is isomorphic to S_5. So $G(E/F) \cong S_5$ is not solvable (by Example 35.19). Therefore, by Theorem 56.4 (really, by Note 1 above), $f(x)$ is not solvable. ∎

Note. The polynomial $f(x)$ of Theorem 56.6 is not in $\mathbb{Q}[x]$. As mentioned in Note 2 above, $f(x) = 2x^5 - 5x^4 + 5 \in \mathbb{Q}[x]$ is not solvable by radicals over $\mathbb{Q}$. Hence we have the result of Niels Henrik Abel of the 1820's. There is an algebraic solution to all first degree polynomial equations, all second degree polynomial equations ("quadratics"), all third degree polynomial equations ("cubics"), and all fourth degree polynomial equations ("quartics"). However, there is no algebraic equation which gives the solution of an arbitrary fifth degree polynomial equation ("quintic"). **Now that's what classical algebra is about!!!**

Revised: 5/1/2015