Section V.9.Appendix.

The General Equation of Degree n

Note. The ancient city of Babylon was located in the southern part of Mesopotamia, about 50 miles south of present day Baghdad, Iraq. Clay tablets containing a type of writing called "cuneiform" survive from Babylonian times, and some of them reflect that the Babylonians had a sophisticated knowledge of certain mathematical ideas, some geometric and some arithmetic. [Page 28 of Jason Socrates Bardi's *The Fifth Postulate: How Unraveling a Two-Thousand-Year-Old Mystery Unraveled the Universe*, John Wiley & Sons: 2009.] An example of a Babylonian algebra problem [see page 1 of Israel Kleiner's *A History of Abstract Algebra*, Birkhäuser: 2007] is the following: "I have added the area and two-thirds of the side of my square and it is 0:35 [35/60 in sexagesimal notation]. What is the side of my square?" The solution is given verbally, as opposed to what we would consider an algebraic solution. In our notation, this problem can be stated as: "Solve for x where $x^2 + (2/3)x = 35/60$." The fact that the Babylonians could solve an equation of this form implies that they could solve any equations of the form $x^2+ax = b$ where $a > 0$ and $b > 0$. This shows that the Babylonians were aware of the quadratic equation. Of course, none of this would be done using equations and the Babylonians would not admit negative numbers as solutions (or as numbers—numbers were thought of as *quantities* and so there was no meaning to a "negative quantity").

Note. Egyptian mathematics was centered more on practical, engineering-related problems than on abstraction. This is evidenced by the Rhind papyrus from 1650 BCE, which gives examples of problems that are basically arithmetical. Problem 21 asks for a solution to $\frac{2}{3}+\frac{1}{15}+x=1$. Much of the content deals with addition of fractions of the form $1/n$. Again, the Egyptians did not use a notation or numerical symbols which we would recognize.

[http://www-history.mcs.st-and.ac.uk/HistTopics/Egyptian_papyri.html]

Note. We now jump way ahead and pick up the story with cubic and quartic equations.

Tartaglia (1500–1557) and Cardano (1501–1576)

(From MacTutor History of Mathematics)

Before the year 1500, the only general polynomial equations which could be solved were linear equations $ax=b$ and quadratic equations $ax^2+bx+c=0$. The use of negative numbers was still not widespread. Around 1515, the Italian Scipione del Ferro was the first to give a solution to a (nontrivial) cubic equation of the form $ax^3+bx=c$, though he never published the result. However, del

Ferro did communicate the result to one of his students (Antonio Maria Fiore) who challenged Niccolò Tartaglia to a public problem solving contest in 1535. Del Ferro only knew how to solve equations of the type given above, but Tartaglia knew how to solve many other types of cubic equations and easily won the contest (and the 16th century equivalent of tenure). Tartaglia reluctantly communicated his result to Gerolamo Cardano. Once he saw the solution, Cardano was able to find a proof for it. At this point (the late 1530s), Ludovico Ferrari, a secretary of Cardano's, learned of the work and was able to find a solution to the quartic equation in 1540 (Ferrari's solution involved a substitution that reduced the quartic equation to a cubic equation). In 1545, Cardano published *Ars Magna* ("*The Great Art*") in which he gave many details on the solutions of the cubic and quartic equations (Tartaglia became enraged at the publication of the cubic result, and this lead to a historical "battle" in the history of math between Tartaglia, del Ferro, and Cardano—a similar battle occurred about 150 years later over priority for the invention of calculus between Newton and Leibniz). The rapid discovery of a solution to the quartic equation following the cubic equation lead those involved to think that solutions of higher degree polynomial equations were on the horizon. [see pages 66–77 of John Derbyshire's *Unknown Quantity: A Real and Imaginary History of Algebra*, Joseph Henry Press: 2006]

Cardano presents dozens of cases for the solutions of cubic and quartic equations. This is due to the fact that negative numbers are still not accepted as "numbers." For example, Cardano would consider the cubic equations $x^3+2x=3$ and $x^3=4x+5$ to be from different "categories." Of course, both are of the form $ax^3+bx+c=0$ if we are allowed to use negative coefficients. So the notation used in the 16th century was not modern, but the solutions to the general equations were known.

For the sake of illustration, let's look at the solution to the cubic equation $ax^3 + bx^2 + cx + d = 0$ in modern notation. The three solutions are:

$$\begin{aligned}
x_1 = &-\frac{b}{3a} - \frac{1}{3a}\sqrt[3]{\frac{1}{2}\left(2b^3 - 9abc + 27a^2d + \sqrt{(2b^3 - 9abc + 27a^2d^2)^2 - 4(b^2 - 3ac)^3}\right)} \\
&-\frac{1}{3a}\sqrt[3]{\frac{1}{2}\left(2b^3 - 9abc + 27a^2d - \sqrt{(2b^3 - 9abc + 27a^2d^2)^2 - 4(b^2 - 3ac)^3}\right)} \\
x_2 = &-\frac{b}{3a} + \frac{1 + \sqrt{-3}}{6a}\sqrt[3]{\frac{1}{2}\left(2b^3 - 9abc + 27a^2d + \sqrt{(2b^3 - 9abc + 27a^2d^2)^2 - 4(b^2 - 3ac)^3}\right)} \\
&+\frac{1 - \sqrt{-3}}{6a}\sqrt[3]{\frac{1}{2}\left(2b^3 - 9abc + 27a^2d - \sqrt{(2b^3 - 9abc + 27a^2d^2)^2 - 4(b^2 - 3ac)^3}\right)} \\
x_3 = &-\frac{b}{3a} + \frac{1 - \sqrt{-3}}{6a}\sqrt[3]{\frac{1}{2}\left(2b^3 - 9abc + 27a^2d + \sqrt{(2b^3 - 9abc + 27a^2d^2)^2 - 4(b^2 - 3ac)^3}\right)} \\
&+\frac{1 + \sqrt{-3}}{6a}\sqrt[3]{\frac{1}{2}\left(2b^3 - 9abc + 27a^2d - \sqrt{(2b^3 - 9abc + 27a^2d^2)^2 - 4(b^2 - 3ac)^3}\right)}
\end{aligned}$$

Note. Of particular historical interest is the impact these equations have had on the acceptance of complex numbers. If we consider the cubic equation $x^3 - 15x - 4 = 0$ [Kleiner, page 7] then we find from the above equations that one solution is $x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}$. This equation can be manipulated by the "usual" algebraic rules with disregard for the fact that $\sqrt{-121}$ makes no sense by 16th century standards. The expression then reduces to $x = 4$ (notice $(4)^3 - 15(4) - 4 = 64 - 60 - 4 = 0$). So the equations above give a meaningful positive solution, even though computation of the solution involves the use of square roots of negatives. This application is where complex numbers gained a hold and eventually became a standard part of "numbers" and mathematics (though not until the 19th century, greatly motivated by Gauss's work). In fact, it is also as solutions to algebraic equations where negative numbers initially gained acceptance.

Note. We now return to Hungerford's approach. Not surprisingly, we want to couch the classical algebraic formula question in the lingo of fields and radical extensions.

Note. We start with a base field K (classically taken to be $\mathbb{Q}$) then consider the field of rational functions $K(t_1, t_2)$ (see Section III.4 and page 233) in indeterminates t_1 and t_2. then for the second degree monic polynomial $x^2 - t_1x + t_2 \in K(t_1, t_2)[x]$ yields the *general quadratic equation* over K, $x^2 - t_1x + t_2 = 0$. Any monic quadratic equation over K can be generated by taking appropriate values of t_1 and t_2. Of course, the solutions to the general quadratic equation (which are in some algebraic closure of $K(t_1, t_2)$) are

$$x = \frac{t_1 \pm \sqrt{t_1^2 - 4 \cdot t_2}}{2 \cdot 1_K}.$$

These solutions can be confirmed y simply substituting them into the general quadratic equation. Notice that the solutions are in $K(u)$ where $u^2 = t_1^2 - 4t_2^2$ (so $K(u)$ is a radical extension of K). Exercise V.9.5 states a concise version of "Cardan's solutions" (more correctly, "Cardano's Solutions") to the general cubic equation; these can also be confirmed by substitution (and lots of classical algebra).

Definition. Let K be a field and $n \in \mathbb{N}$. consider the field $K(t_1, t_2, \ldots, t_n)$ of rational functions over K in the indeterminates $t_1, t_2, \ldots, t_n$. The polynomial

$$p_n(x) = x^n - t_1x^{n-1} + t_2x^{n-2} + \cdots + (-1)^{n-1}t_{n-1}x + (-1)^n t_n \in K(t_1, t_2, \ldots, t_n)[x]$$

is the *general polynomial of degree n over K* and the equation $p_n(x) = 0$ is the *general equation of degree n over K*.

Definition. There is a (algebraic) *formula* for the solution of the general equation of degree n over K provided that this equation is solvable by radicals over the fields $K(t_1, t_2, \ldots, t_n)$.

Note. We have defined things such that we address the existence of a general formula. We have seen in Section V.9 that $x^5 - 4x + 2 = 0$ is not solvable by radicals (over $\mathbb{Q}$). Of course *some* quintics can be solved by radicals. So there is no formula for the solutions to the general quintic equations can be easily solved. Consider, for example, $x^5 - 2x^4 + 2x^3 - 2x^2 + x = 0$. We have:

$$x^5-2x^4+2x^3-2x^2+x = x(x^4-2x^3+2x^2-2x+1) = x((x^4-2x^3+x^2)+(x^2-2x+1))$$

$$= x(x^2+1)(x^2-2x+1) = x(x-i)(x+i)(x-1)^2,$$

so the solutions are 0, i, $-i$, 1, and 1.

Proposition V.9.8. Abel's Theorem.
Let K be a field and $n \in \mathbb{N}$. The general equation of degree n is solvable by radicals only if $n \leq 4$.

Note. If $\text{char}(K) = 0$ then we can replace "only if" with "if and only if." This is because S_n is solvable for $n \leq 4$ by Exercise II.7.10, and then the claim is justified by Corollary V.9.7.

Note. We can also change "only if" to "if and only if" in the case when char$(K) =\neq 0$ by revising the definition of "radical extension."

Alternate Definition. Let K be a field of characteristic $p \neq 0$. F is a *radical extension* of K if there is a finite tower of fields $K = E_0 \subset E_1 \subset \cdots \subset E_n = F$ such that for $1 \leq i \leq n$, $E_i = E_{i-1}(u_i)$ and one of the following is true: (i) $u_i^{m_i} \in E_{i-1}$ for some $m_i \in \mathbb{N}$, or (ii) $u^p - u \in E_{i-1}$.

This claim is to be justified in Exercise V.9.2.

Note. We now present several results which are exercises in Fraleigh's *A First Course In Abstract Algebra*, 7th Edition. These exercises will give us a way to produce specific polynomials for which there is no (algebraic) formula generating the roots.

Fraleigh's Exercise 56.8(a). Prove that if a subgroup H of S_5 contains a cycle of length 5 and a transposition τ, then $H = S_5$. NOTE: This is a generalization of Hungerford's Exercise I.6.4(a).

Proof. Without loss of generality, let the 5 cycle be $(1, 2, 3, 4, 5)$ and let the transposition be $\tau = (1, 2)$. Since H is a group, it contains the following elements (remember to perform the multiplication from right to left):

$$\begin{aligned}
(1,2,3,4,5)(1,2)(1,2,3,4,5)^4 &= (1)(2,3)(4)(5) = (2,3)\\
(1,2,3,4,5)^2(1,2)(1,2,3,4,5)^3 &= (1)(2)(3,4)(5) = (3,4)\\
(1,2,3,4,5)^3(1,2)(1,2,3,4,5)^2 &= (1)(2)(3)(4,5) = (4,5)\\
(1,2,3,4,5)^4(1,2)(1,2,3,4,5) &= (1,5)(2)(3)(4) = (1,5)
\end{aligned}$$

So H contains the transpositions $(1,2)$, $(2,3)$, $(3,4)$, $(4,5)$ and $(5,1)$. Let $a,b \in \{1,2,3,4,5\}$ where $a<b$. Then

$$(a,b) = (a+1,a)(a+2,a+1)\cdots(b-2,b-3)(b-1,b-2)(b-1,b)(b-2,b-1)$$
$$\cdots(a+1,a+2)(a,a+1).$$

So H must contain all transpositions. By Corollary I.6.5, any permutation of $\{1,2,3,4,5\}$ of at least two elements (that is, excluding the identity permutation) is a product of transpositions. Since H includes all transpositions (and the identity) then it must contain all permutations of $\{1,2,3,4,5\}$. That is, $H = S_5$. ∎

Fraleigh's Exercise 56.8(b). Prove that if $f(x)$ is an irreducible polynomial in $\mathbb{Q}[x]$ of degree 5 having exactly two complex and three real zeros, then the group of $f(x)$ over $\mathbb{Q}$ is isomorphic to S_5.

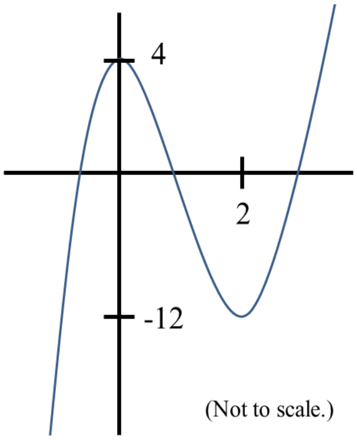
Proof. Let $f(x)$ be such a degree 5 polynomial over $\mathbb{Q}$ and let K be the splitting field of $f(x)$ over $\mathbb{Q}$. Notice that WLOG, $f(x)$ can be monic. By Theorem V.4.2(i), $\mathrm{Aut}_{\mathbb{Q}}(K)$ is isomorphic to some subgroup of S_5.

Let α be a zero of $f(x)$. Then by Theorem V.1.6 (parts (ii) and (iii)), $[\mathbb{Q}(\alpha):\mathbb{Q}] = 5$. By Theorem V.1.2, $[K:\mathbb{Q}] = [K:\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}]$. So 5 divides $[K:\mathbb{Q}]$. Since $f(x)$ is of degree 5 and has exactly 5 roots (that is, 5 distinct roots) then $f(x)$ is a separable polynomial (Definition V.3.10). By Theorem V.3.11 (the (iii) implies (i) part) then K is algebraic and Galois over $\mathbb{Q}$. By the Fundamental Theorem of Galois Theory (Theorem V.2.5(i)), $[K:\mathbb{Q}] = |\mathrm{Aut}_{\mathbb{Q}}(K)|$. So 5 divides $|\mathrm{Aut}_{\mathbb{Q}}(K)|$. By Cauchy's Theorem (Theorem II.5.2) $\mathrm{Aut}_{\mathbb{Q}}(K)$ has an element of order 5. The only elements of order 5 in S_5 are 5 cycles, so $\mathrm{Aut}_{\mathbb{Q}}(K)$ contains (up to isomorphism, at least) a 5 cycle.

Now suppose $a+ib$ is a zero of $f(x)$. Then $a-ib$ is also a zero of $f(x)$ (complex zeros of real polynomials must come in conjugate pairs). The automorphism σ of field $\mathbb{C}$ defined as $\sigma(1)=1$ and $\sigma(i)=-i$ induces an automorphism of K which fixes $\mathbb{Q}$ and satisfies $\sigma(a+ib)=a-ib$ (this is σ restricted to K). Then this restriction of σ is in $\mathrm{Aut}_{\mathbb{Q}}(K)$ and $\sigma^2=\iota$, so σ (up to isomorphism) is a transposition in S_5. So $\mathrm{Aut}_{\mathbb{Q}}(K)\le S_5$ contains a transposition and a 5 cycle. By Fraleigh's Exercise 56.8(a), $\mathrm{Aut}_{\mathbb{Q}}(K)\cong S_5$. ∎

Fraleigh's Exercise 56.8(c). The polynomial $f(x)=2x^5-5x^4+5$ is irreducible in $\mathbb{Q}[x]$, by the Eisenstein Criterion (Theorem III.6.15) with $p=5$. Use Fraleigh's Exercise 56.8(b) and by the contrapositive of Corollary V.9.5, to show that $f(x)=0$ is not solvable by radicals over $\mathbb{Q}$.

Solution. Notice that $f'(x)=10x^4-20x^3=10x^3(x-2)$, so $f'(x)=0$ for $x=0$ and $x=2$. We find by the First Derivative Test that $f(x)$ is increasing for $x\in(-\infty,0]\cup[2,\infty)$ and $f(x)$ is decreasing for $x\in[0,2]$. Since $f(0)=4>0$ and $f(2)=-11<0$, the graph of $f(x)$ is something like:



Notice that $f(x)$ is unbounded below for $x < 0$ and unbounded above for $x > 0$. So (by the Intermediate Value Theorem), f has a real zero in $(-\infty, 0)$, a real zero in $(0, 2)$, and a real zero in $(2, \infty)$. Notice that each of these zeros is of multiplicity 1 (since the derivative is nonzero at these values, whatever they are). So $f(x)$ has three distinct real zeros and (by the Fundamental Theorem of Algebra [Theorem 31.18]) two complex zeros. So by Fraleigh's Exercise 56.8(b), the Galois group of $f(x)$ over $\mathbb{Q}$ is S_5. Now S_5 is not solvable by Corollary II.7.12. Hence, by the contrapositive of Corollary V.9.5, the equation $f(x) = 0$ is not solvable by radicals over $\mathbb{Q}$.

Fraleigh's Exercise 56.9. Find another example of a polynomial over $\mathbb{Q}$ which is not solvable by radicals over $\mathbb{Q}$ (don't just give a multiple of the example of Fraleigh's Exercise 56.8(c)). Use the Eisenstein Criterion to show that your example is in fact irreducible (and give p) and use calculus to show that your example has three real zeros and two complex zeros and then follow Fraleigh's Exercise 56.8(c).

Solution. Consider $f(x) = x^5 - 7x^4 + 7$. Then $f(x)$ is irreducible by the Eisenstein Criterion (Theorem III.6.15) with $p = 7$. Also, $f'(x) = 5x^4 - 28x^3 = x^3(5x - 28)$. So $f'(x) = 0$ for $x = 0$ and $x = 28/5$. We find by the First Derivative Test that $f(x)$ is increasing for $x \in (-\infty, 0] \cup [28/5, \infty)$ and $f(x)$ is decreasing for $x \in [0, 28/5]$. Since $f(0) = 7 > 0$ and $f(28/5) = -1067 - (1842/3125) < 0$ (now you see why Fraleigh chose to use $p = 5$).

As in Fraleigh's Exercise 56.8(c), we have that $f(x)$ is unbounded below for $x < 0$ and unbounded above for $x > 0$. So (by the Intermediate Value Theorem), f has a real zero in $(-\infty, 0)$, a real zero in $(0, 28/5)$, and a real zero in $(28/5, \infty)$.

Notice that each of these zeros is of multiplicity 1 (since the derivative is nonzero at these values, whatever they are). So $f(x)$ has three distinct real zeros and (by the Fundamental Theorem of Algebra [Theorem V.3.19]) two complex zeros. So by Fraleigh's Exercise 56.8(b), the Galois group of $f(x)$ over $\mathbb{Q}$ is S_5. Now S_5 is not solvable by Corollary II.7.12. Hence, by the contrapositive of Corollary V.9.5, the equation $f(x) = 0$ is not solvable by radicals.

Note. A similar analysis (with even messier numbers) reveals that $f(x) = x^5 - 4x + 2$ is also an example of such a polynomial (see Hungerford's page 276).

Note. A more general result related to Fraleigh's Exercise 56.8 is the following from Section V.4:

> **Theorem V.4.12.** If p is prime and f is an irreducible polynomial of degree p over $\mathbb{Q}$ which has precisely two nonreal roots in the field of complex numbers, then the Galois group of f is isomorphic to S_p.

Since S_n is not solvable for $n \geq 5$, then Hungerford's theorem gives a potential way to produce more (prime degree) polynomials which are not solvable by radicals. For example, with $f(x) = x^7 - 4x^6 - 14x^5 + 56x^4 + 48x^3 - 196x^2 - 36x + 202$ we see that f is irreducible by the Eisenstein Criterion (Theorem III.6.15) with $p = 2$. One can verify numerically that f has five real roots (approximately -3.046, -1.765, -1.290, 3.105, and 4.005) and two complex roots (approximately $1.495 \pm 0.326i$). So, if you will accept the impurity of a numerical approximation, this is an example of a 7th degree polynomial equation (a "septic" equation) where the polynomial has associated Galois group S_7 and, therefore, the equation is not solvable by radicals.

Revised: 4/27/2016