Galois-theoretic derivation of the cubic formula

Canonical name	GaloistheoreticDerivationOfTheCubicFormula
Date of creation	2013-03-22 12:10:43
Last modified on	2013-03-22 12:10:43
Owner	djao (24)
Last modified by	djao (24)
Numerical id	9
Author	djao (24)
Entry type	Proof
Classification	msc 12D10
Related topic	GaloisTheoreticDerivationOfTheQuarticFormula

We are trying to find the roots r_1, r_2, r_3 of the polynomial $x^3 + ax^2 + bx + c = 0$. From the equation

$$(x - r_1)(x - r_2)(x - r_3) = x^3 + ax^2 + bx + c$$

we see that

$$\begin{aligned} a &= -(r_1 + r_2 + r_3) \\ b &= r_1 r_2 + r_1 r_3 + r_2 r_3 \\ c &= -r_1 r_2 r_3 \end{aligned}$$

The goal is to explicitly construct a radical tower over the field $k = \mathbb{C}(a, b, c)$ that contains the three roots r_1, r_2, r_3.

Let $L = \mathbb{C}(r_1, r_2, r_3)$. By Galois theory we know that $\mathrm{Gal}(L/\mathbb{C}(a, b, c)) = S_3$. Let $K \subset L$ be the fixed field of $A_3 \subset S_3$. We have a tower of field extensions

$$\begin{tikzcd} L = \mathbb{C}(r_1, r_2, r_3) \arrow[d, dash, "A_3"'] \\ K = \,? \arrow[d, dash, "S_3/A_3"'] \\ k = \mathbb{C}(a, b, c) \end{tikzcd}$$

which we know from Galois theory is radical. We use Galois theory to find K and exhibit radical generators for these extensions.

Let $\sigma := (123)$ be a generator of $\mathrm{Gal}(L/K) = A_3$. Let $\omega = e^{2\pi i/3} \in \mathbb{C} \subset L$ be a primitive cube root of unity. Since ω has norm 1, Hilbert's Theorem 90 tells us that $\omega = y/\sigma(y)$ for some $y \in L$. Galois theory (or Kummer theory) then tells us that $L = K(y)$ and $y^3 \in K$, thus exhibiting L as a radical extension of K.

The proof of Hilbert's Theorem 90 provides a procedure for finding y, which is as follows: choose any $x \in L$, form the quantity

$$\omega x + \omega^2 \sigma(x) + \omega^3 \sigma^2(x);$$

then this quantity automatically yields a suitable value for y provided that it is nonzero. In particular, choosing $x = r_2$ yields

$$y = r_1 + \omega r_2 + \omega^2 r_3.$$

and we have $L = K(y)$ with $y^3 \in K$. Moreover, since $\tau := (23)$ does not fix y^3, it follows that $y^3 \notin k$, and this, combined with $[K : k] = 2$, shows that $K = k(y^3)$.

Set $z := \tau(y) = r_1 + \omega^2 r_2 + \omega r_3$. Applying the same technique to the extension K/k, we find that $K = k(y^3 - z^3)$ with $(y^3 - z^3)^2 \in k$, and this exhibits K as a radical extension of k.

To get explicit formulas, start with $y^3 + z^3$ and $y^3 z^3$, which are fixed by S_3 and thus guaranteed to be in k. Using the reduction algorithm for symmetric polynomials, we find

$$\begin{aligned} y^3 + z^3 &= -2a^3 + 9ab - 27c \\ y^3 z^3 &= (a^2 - 3b)^3 \end{aligned}$$

Solving this system for y and z yields

$$\begin{aligned} y &= \left(\frac{-2a^3 + 9ab - 27c + \sqrt{(2a^3 - 9ab + 27c)^2 + 4(-a^2 + 3b)^3}}{2} \right)^{1/3} \\ z &= \left(\frac{-2a^3 + 9ab - 27c - \sqrt{(2a^3 - 9ab + 27c)^2 + 4(-a^2 + 3b)^3}}{2} \right)^{1/3} \end{aligned}$$

Now we solve the linear system

$$\begin{aligned} a &= -(r_1 + r_2 + r_3) \\ y &= r_1 + \omega r_2 + \omega^2 r_3 \\ z &= r_1 + \omega^2 r_2 + \omega r_3 \end{aligned}$$

and we get

$$\begin{aligned} r_1 &= \frac{1}{3}(-a + y + z) \\ r_2 &= \frac{1}{3}(-a + \omega^2 y + \omega z) \\ r_3 &= \frac{1}{3}(-a + \omega y + \omega^2 z) \end{aligned}$$

which expresses r_1, r_2, r_3 as radical expressions of a, b, c by way of the previously obtained expressions for y and z, and completes the derivation of the cubic formula.