Galois-theoretic derivation of the quartic formula

Canonical name	GaloistheoreticDerivationOfTheQuarticFormula
Date of creation	2013-03-22 12:34:35
Last modified on	2013-03-22 12:34:35
Owner	djao (24)
Last modified by	djao (24)
Numerical id	9
Author	djao (24)
Entry type	Proof
Classification	msc 12D10
Related topic	GaloisTheoreticDerivationOfTheCubicFormula
Defines	resolvent cubic

Let $x^4 + ax^3 + bx^2 + cx + d$ be a general polynomial with four roots r_1, r_2, r_3, r_4, so $(x-r_1)(x-r_2)(x-r_3)(x-r_4) = x^4 + ax^3 + bx^2 + cx + d$. The goal is to exhibit the field extension $\mathbb{C}(r_1, r_2, r_3, r_4)/\mathbb{C}(a, b, c, d)$ as a radical extension, thereby expressing r_1, r_2, r_3, r_4 in terms of a, b, c, d by radicals.

Write N for $\mathbb{C}(r_1, r_2, r_3, r_4)$ and F for $\mathbb{C}(a, b, c, d)$. The Galois group $\mathrm{Gal}(N/F)$ is the symmetric group S_4, the permutation group on the four elements $\{r_1, r_2, r_3, r_4\}$, which has a composition series

$$1 \lhd \mathbb{Z}/2 \lhd V_4 \lhd A_4 \lhd S_4,$$

where:

- A_4 is the alternating group in S_4, consisting of the even permutations.
- $V_4 = \{1, (12)(34), (13)(24), (14)(23)\}$ is the Klein four-group.
- $\mathbb{Z}/2$ is the two–element subgroup $\{1, (12)(34)\}$ of V_4.

Under the Galois correspondence, each of these subgroups corresponds to an intermediate field of the extension N/F. We denote these fixed fields by (in increasing order) K, L, and M.

We thus have a tower of field extensions, and corresponding automorphism groups:

$$\begin{tikzcd}
\text{Subgroup} & \text{Fixed field} \\
1 & N \arrow[d, dash] \\
\mathbb{Z}/2 & M \arrow[d, dash] \\
V & L \arrow[d, dash] \\
A_4 & K \arrow[d, dash] \\
S_4 & F
\end{tikzcd}$$

By Galois theory, or Kummer theory, each field in this diagram is a radical extension of the one below it, and our job is done if we explicitly find what the radical extension is in each case.

We start with K/F. The index of A_4 in S_4 is two, so K/F is a degree two extension. We have to find an element of K that is not in F. The easiest such element to take is the element Δ obtained by taking the products of the differences of the roots, namely,

$$\Delta := \prod_{1\leq i<j\leq 4} (r_i - r_j) = (r_1 - r_2)(r_1 - r_3)(r_1 - r_4)(r_2 - r_3)(r_2 - r_4)(r_3 - r_4).$$

Observe that Δ is fixed by any even permutation of the roots r_i, but that $\sigma(\Delta) = -\Delta$ for any odd permutation σ. Accordingly, Δ^2 is actually fixed by all of S_4, so:

- $\Delta \in K$, but $\Delta \notin F$.
- $\Delta^2 \in F$.
- $K = F[\Delta] = F[\sqrt{\Delta^2}]$, thus exhibiting K/F as a radical extension.

The element $\Delta^2 \in F$ is called the *discriminant* of the polynomial. An explicit formula for Δ^2 can be found using the reduction algorithm for symmetric polynomials, and, although it is not needed for our purposes, we list it here for reference:

$$\begin{aligned}\Delta^2 \quad = \quad & 256d^3 - d^2(27a^4 - 144a^2b + 128b^2 + 192ac) - \\ & c^2(27c^2 - 18abc + 4a^3c + 4b^3 - a^2b^2) - \\ & 2d(abc(9a^2 - 40b) - 2b^3(a^2 - 4b) - 3c^2(a^2 - 24b)).\end{aligned}$$

Next up is the extension L/K, which has degree 3 since $[A_4 : V_4] = 3$. We have to find an element of N which is fixed by V_4 but not by A_4. Luckily, the form of V_4 almost cries out that the following elements be used:

$$\begin{aligned} t_1 &:= (r_1 + r_2)(r_3 + r_4) \\ t_2 &:= (r_1 + r_3)(r_2 + r_4) \\ t_3 &:= (r_1 + r_4)(r_2 + r_3) \end{aligned}$$

These three elements of N are fixed by everything in V_4, but not by everything in A_4. They are therefore elements of L that are not in K. Moreover, every permutation in S_4 permutes the set $\{t_1, t_2, t_3\}$, so the cubic polynomial

$$\Phi(x) := (x - t_1)(x - t_2)(x - t_3)$$

actually has coefficients in F! In fancier language, the cubic polynomial $\Phi(x)$ defines a cubic extension E of F which is linearly disjoint from K, with the composite extension EK equal to L. The polynomial $\Phi(x)$ is called the *resolvent cubic* of the quartic polynomial $x^4 + ax^3 + bx^2 + cx + d$. The coefficients of $\Phi(x)$ can be found fairly easily using (again) the reduction algorithm for symmetric polynomials, which yields

$$\Phi(x) = x^3 - 2bx^2 + (b^2 + ac - 4d)x + (c^2 + a^2d - abc). \tag{1}$$

Using the cubic formula, one can find radical expressions for the three roots of this polynomial, which are t_1, t_2, and t_3, and henceforth we assume radical expressions for these three quantities are known. We also have $L = K[t_1]$, which in light of what we just said, exhibits L/K as an explicit radical extension.

The remaining extensions are easier and the reader who has followed to this point should have no trouble with the rest. For the degree two extension M/L, we require an element of M that is not in L; one convenient such element is $r_1 + r_2$, which is a root of the quadratic polynomial

$$(x - (r_1 + r_2))(x - (r_3 + r_4)) = x^2 + ax + t_1 \in L[x] \tag{2}$$

and therefore equals $(-a + \sqrt{a^2 - 4t_1})/2$. Hence $M = L[r_1 + r_2] = L[(-a + \sqrt{a^2 - 4t_1})/2]$ is a radical extension of L.

Finally, for the extension N/M, an element of N that is not in M is of course r_1, which is a root of the quadratic polynomial

$$(x - r_1)(x - r_2) = x^2 - (r_1 + r_2)x + r_1r_2. \tag{3}$$

Now, $r_1 + r_2$ is known from the previous paragraph, so it remains to find an expression for r_1r_2. Note that r_1r_2 is fixed by (12)(34), so it is in M but not in L. To find it, use the equation $(t_2 + t_3 - t_1)/2 = r_1r_2 + r_3r_4$, which gives

$$(x - r_1r_2)(x - r_3r_4) = x^2 - \frac{(t_2 + t_3 - t_1)}{2}x + d$$

and, upon solving for r_1r_2 with the quadratic formula, yields

$$r_1r_2 = \frac{(t_2 + t_3 - t_1) + \sqrt{(t_2 + t_3 - t_1)^2 - 16d}}{4} \tag{4}$$

$$r_3r_4 = \frac{(t_2 + t_3 - t_1) - \sqrt{(t_2 + t_3 - t_1)^2 - 16d}}{4} \tag{5}$$

We can then use this expression, combined with Equation (**??**), to solve for r_1 using the quadratic formula. Perhaps, at this point, our poor reader needs a summary of the procedure, so we give one here:

1. Find t_1, t_2, and t_3 by solving the resolvent cubic (Equation (**??**)) using the cubic formula,

2. From Equation (**??**), obtain

$$\begin{aligned} r_1 + r_2 &= \frac{(-a + \sqrt{a^2 - 4t_1})}{2} \\ r_3 + r_4 &= \frac{(-a - \sqrt{a^2 - 4t_1})}{2} \end{aligned}$$

3. Using Equation (**??**), write

$$\begin{aligned} r_1 &= \frac{(r_1 + r_2) + \sqrt{(r_1 + r_2)^2 - 4(r_1 r_2)}}{2} \\ r_2 &= \frac{(r_1 + r_2) - \sqrt{(r_1 + r_2)^2 - 4(r_1 r_2)}}{2} \\ r_3 &= \frac{(r_3 + r_4) + \sqrt{(r_3 + r_4)^2 - 4(r_3 r_4)}}{2} \\ r_4 &= \frac{(r_3 + r_4) - \sqrt{(r_3 + r_4)^2 - 4(r_3 r_4)}}{2} \end{aligned}$$

   where the expressions r_1+r_2 and r_3+r_4 are derived in the previous step, and the expressions $r_1 r_2$ and $r_3 r_4$ come from Equation (**??**) and (**??**).

4. Now the roots r_1, r_2, r_3, r_4 of the quartic polynomial $x^4+ax^3+bx^2+cx+d$ have been found, and we are done!