Galois Theory – Historical Perspective

Bryan Lu

May 2022

0 Foreword

These are some notes on Galois theory following H. M. Edwards' *Galois Theory*. Galois theory is an overlooked subject in Cornell's algebra sequence – it's only given a passing mention in MATH 4340, the honors abstract algebra course, and it's kind of a shame it's treated this way. At its heart is a nice connection between fields and groups and I feel like it's a big part of why one would want to study fields in the first place. I also think Galois theory is important in leveling up an understanding of number theory as well as dealing with fields and number systems in general beyond just the integers, so I think it's useful in algebraic NT...? I really don't know much more in this regard so I should stop talking lol but those are my thoughts on why it's important, at least.

I also think that there's a lot of historical mystique around the field as well – a lot of people know the story of how Evariste Galois was shot and killed in a duel at age 21, and the night before he died he feverishly wrote down the groundwork for this really amazing theory. What a story, right? I kinda like Edwards' book because the smoke and mirrors are cleared here – you get the benefit of the historical context in which Galois was working, and also understand the angle at which he was coming from when he wrote all that stuff without losing the modern interpretation of the results. I don't think this is a very standard treatment of the subject at all, but I think it's fun nonetheless and will do some mixing in with Dummit and Foote as needed.

Some prerequisites – while you don't technically need to have any background in algebra to understand the book, I will assume familiarity with group theory in these notes. These notes are a distillation of the important developments in the field's history and while the book does go out of its way to also explain groups and stuff, I won't. There's also the whole story about solving the cubic/quartic with Cardano and Tartaglia and Ferrari and del Ferro which is commonly used as historical setup for Abel-Ruffini, a theorem often discussed in a treatment Galois theory – if you're interested in the story, I won't rehash it here as so many people do it, but if you don't know about it you should find out! Veritasium has a really nice popular depiction of it and he does a much better job than I ever could so I'll assume you'll get the story from elsewhere and I won't have to talk about it.

1 History of Solving Polynomial Equations

A brief history of solving polynomial equations (of degree higher than 1):

- The Babylonians knew how to solve quadratics! This is akin to Po-Shen Loh's method of solving quadratics today – conceiving it instead as a puzzle in which you have to figure out two numbers (the roots of a quadratic) given only their sum and product.
- Not a lot of progress on cubics and quartics until the aforementioned developments by del Ferro/Cardano/Tartaglia in the 16th century – there's a surprising amount of drama and tea here. The main ideas:

  - Depressing the cubic – take cubics of the form $x^3 + ax^2 + bx + c$ and introduce the change of variables $y = x - \frac{a}{3}$, which eliminates the quadratic term. Leaves you with an equation of the form $y^3 + py + q$.
  - Guess that $y = m - n$. Substituting, you can see that a good heuristic for the solution is that $3mn = p$, $m^3 - n^3 + q = 0$. Note that $27m^6 - 27m^3n^3 + 27m^3q = 0$ as well, but $27m^3n^3 = p^3$, so you actually have a quadratic in m^3 now, allowing you to solve for m and n now, and then unwinding to get y and then x.

- Quartics would fall very shortly after due to Ferrari. This is more undisputed I think? Again, just the main ideas:
  - Depress the quartic now – introduce the change of variables $y = x - \frac{a}{4}$ for the quartic $x^4 + ax^3 + bx^2 + cx + d$, which leaves a new quartic $y^4 + py^2 + qy + r$.
  - Introduce a new variable z, and consider $(y^2 + z)^2 = y^4 + 2y^2z + z^2 = (-p + 2z)y^2 - qy - r + z^2$. Heuristically, we want to be able to take the square root of the RHS. This means that this quadratic in y actually has to have a single root, so this happens when $q^2 - 4(-p + 2z)(z^2 - r) = 0$. This gives a cubic in z that can be solved!
  - Solve for z using the procedure for a cubic. If z is now chosen appropriately, we get that $(y^2 + z) = \pm\sqrt{-p + 2z}\left(y - \frac{q}{2(-p+2z)}\right)$, which gives a quadratic that can now be solved.
- Abel shows in the 19th century (c. 1820) that it's impossible to solve qunitics or higher in general form in the same way as above. (This proof is not based in Galois theory, but uses some of the techniques mentioned in future sections.)
  Note that this is about a 300-year gap without seemingly much progress on this problem! What were people up to in that time?

1.1 Fundamental Theorem on Symmetric Polynomials, Vieta's Formulas, Newton's Sums

One of the most important developments in algebra (for us) in the time between the time of the Great Italian War of Cubics and Quartics and Abel's big contribution in the early 1800s is a development in the theory of symmetric polynomials.

First, I feel like I have to mention Francois Viete here, along with Vieta's formulas – discovered in the late 16th century. I do need to provide a definition first –

Definition 1

The ***k*th elementary symmetric polynomial** on n variables $x_1, x_2, \ldots, x_n$, $e_k(x_1, x_2, \ldots, x_n)$ is the sum of all $\binom{n}{k}$ terms $x_{i_1}x_{i_2}\ldots x_{i_k}$ $(i_1 < i_2 < \cdots < i_k)$ where all of the $i_j \in [n]$.

Viete figured out how to express elementary symmetric polynomials in the roots of a polynomial in terms of the coefficients of that polynomial:

Theorem 2 (Vieta's Formulas)

If a polynomial $a_nx^n + \cdots + a_1x + a_0$ has roots $r_1, r_2, \ldots, r_n$, then the elementary symmetric polynomials are expressible in terms of the roots. In particular, $e_k(r_1, r_2, \ldots, r_n) = (-1)^k\frac{a_{n-k}}{a_n}$.

The proof of this theorem is fairly straightforward – just expand $a_n(x-r_1)\dots(x-r_n)$ and it sort of just appears combinatorially.

Later on, towards the end of the 17th century, it's clear that Newton knew how to express many different symmetric sums of roots of a polynomial in terms of its roots. His results were many specific cases of this (important!) theorem:

Definition 3

A polynomial in n variables $P(x_1,\dots,x_n)$ is **symmetric** if interchanging any two x_i and x_j does not change the polynomial.

Theorem 4 (Fundamental Theorem on Symmetric Polynomials)

Every symmetric polynomial (in n variables) can be expressed as a polynomial in the elementary symmetric polynomials (in n variables) e_k.

This theorem was widely cited/known before the time of Galois, but the first known proof of this statement comes to us from the 19th century. Oops. We'll prove it here too:

Proof. We proceed by induction on n, the number of variables. The theorem is sort of silly for $n=1$, so that'll be our base case. (With one variable, the only symmetric polynomial you can really have is just a polynomial, which is clearly a polynomial in that one variable.)

Our inductive hypothesis will be that the every symmetric polynomial in $n-1$ variables can be expressed as a polynomial in the elementary symmetric polynomials in $n-1$ variables. Now, let's say we have a symmetric polynomial in n variables, $F(x_1,x_2,\dots,x_n)$. Let's split F into powers of x_n, and suppose that the highest degree of x_n that appears is m, so F can be decomposed:

$$F(x_1,x_2,\dots,x_n) = F_0 + F_1x_n + F_2x_n^2 + \dots F_mx_n^m.$$

where now each of the F_ks for $0\le k\le m$ have to be symmetric polynomials in $x_1,\dots,x_{n-1}$. This must be true as if some F_i were not symmetric in the $x_1,\dots,x_{n-1}$, then F would not be either. Therefore, we can apply the inductive hypothesis to each of the F_ks, so we know that they can all be written as a sum of elementary symmetric polynomials $e_k^{(n-1)}$ in $x_1,\dots,x_{n-1}$. As such, $F_k(x_1,\dots,x_{n-1}) = f_k(e_1^{(n-1)},\dots,e_{n-1}^{(n-1)})$ for a different polynomial f_k in the $e_k^{(n-1)}$s.

We're not done yet though, we still need to write F in terms of the elementary symmetric polynomials in $x_1,\dots,x_n$, $e_k^{(n)}$. Let's get one step closer now by relating the $e_k^{(n)}$ to $e_k^{(n-1)}$ in the following way:

$$\begin{aligned}
e_1^{(n)} &= e_1^{(n-1)} + x_n\\
e_2^{(n)} &= e_2^{(n-1)} + x_ne_1^{(n-1)}\\
e_3^{(n)} &= e_3^{(n-1)} + x_ne_3^{(n-1)}\\
&\vdots\\
e_{n-1}^{(n)} &= e_{n-1}^{(n-1)} + x_ne_{n-2}^{(n-1)}\\
e_n^{(n)} &= x_ne_{n-1}^{(n-1)}
\end{aligned}$$

In particular, we can then write $e_k^{(n-1)}$ as a polynomial in x_n and the $e_k^{(n)}$s (this can easily be seen by induction). This allows us to rewrite each of the $f_k(e_1^{(n-1)},\dots,e_{n-1}^{(n-1)})$ as polynomials in $e_k^{(n)}$ and x_n, which will require us to recollect terms.

We can reduce this further – by backsubstituting each of the last equations from the end into the last, we can find the following identity for $e_n^{(n)}$ in terms of x_n and lower $e_k^{(n)}$ for $k < n$:

$$e_n^{(n)} - x_n e_{n-1}^{(n)} + x_n^2 e_{n-2}^{(n)} + \cdots + (-1)^n x_n^n = 0.$$

This allows us to reduce the maximal degree until all terms have powers of x_n less than n, so we can write

$$F(x_1, \ldots, x_n) = h_0(e_1^{(n)}, \ldots, e_n^{(n)}) + h_1(e_1^{(n)}, \ldots, e_n^{(n)})x_n + \cdots + h_{n-1}(e_1^{(n)}, \ldots, e_n^{(n)})x_n^{n-1}.$$

We now want to show that all of the h_is for $i > 0$ are identically 0 to finish the induction.

Recall again that F is a symmetric polynomial, so swapping x_n with any other x_i should leave the same result. Since each of the h_ks are polynomials in elementary symmetric polynomials, swapping x_n and any other x_i would also leave them the same, so this swap would only change the powers of x_n. If we do this for every other variable, we get the following system of equations:

$$\begin{aligned} F(x_1, \ldots, x_n) &= h_0 + h_1 x_1 + \cdots + h_{n-1} x_1^{n-1} \\ F(x_1, \ldots, x_n) &= h_0 + h_1 x_2 + \cdots + h_{n-1} x_2^{n-1} \\ &\vdots \\ F(x_1, \ldots, x_n) &= h_0 + h_1 x_n + \cdots + h_{n-1} x_n^{n-1} \end{aligned}$$

We can view this as a matrix equation:

$$\begin{bmatrix} F(x_1, \ldots, x_n) \\ F(x_1, \ldots, x_n) \\ \vdots \\ F(x_1, \ldots, x_n) \end{bmatrix} = \begin{bmatrix} 1 & x_1 & \ldots & x_1^{n-1} \\ 1 & x_2 & \ldots & x_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \ldots & x_n^{n-1} \end{bmatrix} \begin{bmatrix} h_0 \\ h_1 \\ \vdots \\ h_{n-1} \end{bmatrix}.$$

Let the matrix in this equation be $V(x_1, \ldots, x_n)$. Note that $V\vec{\mathbf{x}} = \begin{bmatrix} F(x_1,\ldots,x_n) \\ F(x_1,\ldots,x_n) \\ \vdots \\ F(x_1,\ldots,x_n) \end{bmatrix}$ has another solution, namely $\vec{\mathbf{x}} = \begin{bmatrix} F(x_1,\ldots,x_n) \\ 0 \\ \vdots \\ 0 \end{bmatrix}$. However, note that V is invertible in the general case – we can show this by showing $\det V \neq 0$ by induction on the number of variables. (In particular, the determinant of V is called the **Vandermonde determinant**, and it's zero iff two of the x_is are equal.) Therefore, the system has a unique solution and therefore all of the h_is for $i > 0$ must be identically 0.

(Another way to finish this off – consider the polynomial $H(y) = -F(x_1, \ldots, x_n) + h_0 + h_1 y + \cdots + h_{n-1} y^{n-1}$, which has n roots at $x_1, x_2, \ldots, x_n$, so it must be divisible by $\prod_{j=1}^{n}(y - x_n)$. Looking at the degree, however, this is only possible if $H(y) = 0$, which implies the same result).

Therefore, $F(x_1, \ldots, x_n) = h_0(e_1^{(n)}, \ldots, e_n^{(n)})$, so the symmetric polynomial F is expressible as a polynomial in the elementary symmetric polynomials in n variables. By induction, then, the statement holds for all $n \geq 1$, as desired. □

Remark. *Newton's sums* are a particular case of this theorem, i.e. when $F(x_1, \ldots, x_n) = x_1^k + \cdots + x_n^k$. Call this polynomial the kth power sum of the x_is, P_k. The case of the fundamental theorem on symmetric polynomials that is attributed to Newton is a formula for P_k in terms of the elementary symmetric polynomials:

$$P_k = P_{k-1}e_1 - P_{k-2}e_2 + \cdots + (-1)^k P_1 e_{k-1} + (-1)^{k+1} k e_k.$$

This is useful for finding the sum of the kth powers of the roots of a polynomial recursively.

As a corollary, we now get that **any symmetric polynomial in the roots of a polynomial is expressible in terms of the coefficients of that polynomial**. This now just follows from combining Vieta's Formulas and the fundamental theorem on symmetric polynomials. This will turn out to be a good motivator for parts of Galois theory down the line when we introduce group actions.

2 Lagrange Resolvents

Let's introduce a new way to go about solving polynomial equations (due to Vandermonde and Lagrange) in the late 18th century, now involving the roots of unity. First, let's introduce the following example for quadratics.

Suppose we have a quadratic with roots x and y. Then we claim that the expression $\frac{1}{2}((x+y) \pm \sqrt{(x-y)^2})$ takes on both of the values of the roots. If we take the positive branch, then $\frac{1}{2}(x+y+x-y) = x$, and on the negative branch, $\frac{1}{2}(x+y-(x-y)) = y$. Therefore, in theory, all we would need to do is just evaluate $x+y$ (using Vieta) and $(x-y)^2$ (some other way) and we'd have solved the quadratic. Indeed, we can get $(x-y)^2$ from $(x+y)^2 - 4xy$, which returns us the familiar quadratic formula when we write these expressions in the coefficients of the quadratic.

Okay, that was a little silly, but we can actually do this for higher-degree polynomials too, we just have to use different roots of unity. For a cubic, if $\omega = e^{\frac{2\pi i}{3}}$, then we should consider the quantity

$$\frac{1}{3}[(x+y+z) + ((x+\omega y+\omega^2 z)^3)^{\frac{1}{3}} + ((x+\omega^2 y+\omega z)^3)^{\frac{1}{3}}].$$

Here we get nine different values upon choosing different branches for the evaluation of the cube roots, only three of which actually produce solutions (in particular, these three are taking no additional factors of ω on either term, and then putting ω on one and ω^2 on the other, in either order).

Is this even possible to evaluate? Technically, yes – if we let $u = (x+\omega y+\omega^2 z)^3$ and $v = (x+\omega^2 y+\omega z)^3$, then $u+v$ and uv are symmetric in x, y, z, which means that we can use the results from the previous section to evaluate them both. Note that if we swap y and z, both quantities are invariant, and also cyclic permutations (xyz) also leave both invariant, and these generate all permutations of x, y, z. As such, it's theoretically possible, but still maybe not great because we still have the issue of getting 9 solutions, but only a third are actually the ones we want. Can we do better?

This first method is due to Vandermonde in 1770 (same guy whose name appears in the determinant in the previous section, and in Vandermonde's identity from combinatorics, but that's maybe it[?]), but Lagrange a little later towards the end of the 18th century (c. 1790) developed a better way using a similar idea.

3 Gauss and Cyclotomic Polynomials

We've been discussing the roots of unity when we introduced Lagrange resolvents as a new way to

A *cyclotomic polynomial* is a