Hidden Premises in Galois Theory

Timothy W. Jones

November 6, 2022

Abstract

This is a primer for Chapter 3 of Hadlock's book *Field Theory and Its Classical Problems*: Solution by Radicals. We take a rather naïve perspective and consider the linear and quadratic cases afresh and evolve what is really met by solving a polynomial by radicals. There are what we consider to be several hidden premises that some students might be subconsciously puzzled about.

Introduction

Consider solving the first degree polynomial $ax + b = 0$. What could be simpler? There are however complexities that underlie such a concept. Are there specific techniques or rules that are to be followed, other rules not being allowed? This seems naïve to even consider; just isolate the x by doing the same arithmetic operation to both sides; arrive at $x = -b/a$. But this procedure embeds the assumption that one is to use arithmetic operations on the coefficients of this polynomial whereas Galois theory we will show doesn't confine allowed procedures to be just these manipulations. We will develop this hidden premise.

Another hidden premise resides in the difference between an expression and a formula. We will show that all polynomials will have all roots that can be given as expressions (ultimately this means elements of a final sequence of field extensions). To give a flavor of what we are talking about consider $x - a = 0$. The expression $x = a$ gives a solution to this polynomial, but it does not give a formula for all linear polynomials. It does give a formula for linear polynomials of the form $x - a = 0$, a subset of all linear polynomials.

We will show that *solution by radicals* means a general formula (not just expressions) for all polynomials of a given degree.

Referring to the arithmetic steps used to solve (find a formula for all degree one polynomials), we used a *finite* number of algebraic manipulations. Does this mean that any method that can be executed in a finite number of steps is allowed and if any such method yields a solution in all cases then the polynomial with a given degree is solved or solvable? To once again get the flavor of this idea, consider that the rational numbers are countable, that is there exists a one-to-one and onto mapping between natural numbers and rational numbers. There are explicit functions. So, given that a and b are integers (a premise to general polynomials assumed in this context) for all linear polynomials we can *search* for a solution by enumerating all p/q rational numbers until we find the solution. This searching idea is true for all polynomials; that is all roots to all polynomials will have roots that can be found by enumeration of all possible solutions. We will show that in this sense all polynomials can be solved and then we will clarify this seeming puzzle.

Allowed Methods

One might assume that the rules (the methods allowed) are to start with the coefficients and use arithmetic operations (field operations) and the taking of roots, but this can't be the case; it is too limiting. Indeed, as Hadlock develops in his problems, the solutions to a cubic polynomial involves substitutions that reduce the cubic to a quadratic (page 126 and 279). Can substitutions distill to operations? Not really. One can substitute the answer, a root, for x but this is an absurdity.

Consider $z^5 = k$, k a constant. The roots are just the fifth roots of k in the complex plane. In specifying these roots, I will use trigonometric functions, sin and cos, but where in the lexicon of allowed arithmetic operations do these occur? The next sections resolves this puzzle.

Expressions Versus Formulas

It must be the case that every polynomial has all its roots in the form of expressions that are defined by being elements of a field. The field is the final

field in a nesting sequence of radical extensions from the rational numbers. That is the roots of a polynomial of any degree must consist of expressions that involve some sequence of arithmetic operations and radicals that could involve any integers, not necessarily the coefficients: Sections 3.1 and 3.2. Every polynomial has such a sequence, but the splitting field might not reside in its final field.

It must be the case that whereas all roots have an expression (a right hand side) of the equivalent of quadratic formula (one of its expressions), the expressions do not yield a general formula for general degree five and greater polynomials. One can also get this result from a combination of the fundamental theorem of algebra, the root form (we'll call it) of a polynomial, and symmetric coefficients that relate these. So, by the FTA roots exists, so $p(x) = (x - r_1)(x - r_2) \dots (x - r_n)$ and so the coefficients are the fundamental symmetric functions that combine these roots to give integers, the coefficients. The only way an expression for a root could not involve arithmetic combinations with radicals is if it was a transcendental number (see a later section) – which by virtue of being a root of an integer polynomial it isn't.

The allowed methods are any methods including exhaustive searches of all possible expressions of the right form. As algebraic numbers are countable, these searches will always be successful, but (here it is) they will not yield unique expressions that are general formulas for roots. Hadlock points this out albeit in a round about way: he gives examples of solvable polynomials and unsolvable polynomials in Section 3.7. A little caveat that could be added is *solvable in a certain way* that applies to all polynomials of a given degree – not using searches!

Finite Steps Clarified

Could we specify as our allowed step for solving all polynomials of arbitrary degree the following: enumerate all possible algebraic numbers, feeding them into our given polynomial and if a zero pops out we found a root? I say yes. But here is a slight catch: we will not have in the end a finite list of expressions for roots for degree greater than or equal to five. We will have infinitely many expressions for roots – no formula.

Other observations

Facts not given by Hadlock (and other books on solutions of polynomials by radicals) are that non-transcendental, irrational numbers are countable – they are all the irrational algebraic numbers and they have a certain form, namely they are elements of the rational field extended using a radical, a $\sqrt[r]{m}$ or the last of a finite number of such extensions. Given any such number we can make it the root of a polynomial. The reverse problem is the rub.

A historical note of interest: Galois (1811-1832), Cantor (1845-1918). In 1874 Cantor proved transcendental numbers are uncountable. Apparently, Euler (1707-1783) was the first mathematician to coin *algebraic* numbers. This is all to say that the following observations may be new – a easy update, if correct.

The Table 1 gives all possible field extensions pertinent to Galois theory. Each field extension $\mathbf{Q}[\sqrt[r]{m}]$ is countable and can be nested in any other such field extension. A method used to show rational numbers are countable can be mimicked here to show all such field extensions and their nesting combinations are countable. Starting at $B2$, spreadsheet referencing, and the first number in this countable field, we next go to $C2$ next door and count the first and second element of its field and add the second element of all previous fields, then zig-zagging its down and over to $B3$ and we count the first three of its field and re-tracing count the third element of all previous fields. This seems to traverse all of these fields and provides a searching mechanism for finding roots. Countable unions of countable sets are countable [3].

	A	B	C	D	E	F	G
1		2	3	4	5	6	...
2	2	$\sqrt{2}$	$\sqrt[3]{2}$	$\sqrt[4]{2}$	$\sqrt[5]{2}$	...	
3	3	$\sqrt{3}$	$\sqrt[3]{3}$	$\sqrt[4]{3}$	$\sqrt[5]{3}$	...	
4	4	$\sqrt{4}$	$\sqrt[3]{4}$	$\sqrt[4]{4}$	$\sqrt[5]{4}$	...	
$\vdots$							

Table 1: All radical field extensions allowed in Galois theory.

Shocking Transcendental Numbers

There appear to be algebraic looking numbers that can't solve an integer polynomial. So, for example, setting

$$r = \sqrt{\sqrt{5} + \sqrt[3]{7}}$$

and taking powers in an obvious way, one arrives at

$$(r^2 - \sqrt{5})^3 - 7 = 0,$$

implying that r can't be a root of an integer polynomial. It must be transcendental! Shocker of shockers this may mean that π might be expressible as a root of some such non-integer polynomial. These irrationals (expressions with arbitrary combinations of radicals of various indices) are, in some books (I think) referred to as *surds* [2]. No book that I've read has ever stated that some surds are transcendental numbers.

Certain types of nesting do always give roots of integer polynomials. So, for example, setting

$$r = \sqrt{2 + \sqrt{3 + \sqrt{5}}},$$

and once again taking powers in an obvious way:

$$((r^2 - 2)^2 - 3))^2 - 5 = 0,$$

implying that r is the root of an integer polynomial. We are using polynomials of the same degree with different coefficients have different roots. This follows as polynomials are well defined functions.

Bad Formulas

A formula (a bad one) for the roots of any nth degree integer polynomial is $r \in \{1, 2, \ldots, n\}$, that is the roots are just the natural numbers 1 through the degree of the polynomial, n. This will be correct for some polynomials and it will not involve the coefficients of that polynomial. Certainly we can show the linear, quadratic, cubic, and quartic cases have formulas that encompass these polynomials. We can also generate polynomials (rather trivially) that have roots not given by this formula. At degree 5 if we can show that all formulas that solve these polynomials can not also solve another of some type then there is no formula for all. Maybe there is an easier way than Galois to get this result.

Conclusion

It is in no way mysterious that formulas for all roots of large degree polynomials are possible. It is essentially that roots are deeply encrypted in coefficients and no single method can pop them out. For degree n there are n symmetric polynomials that are every more complicated. It is no wonder that at some moderate degree like five, no single method can be used.

A quantum computer might be able to find expressions for roots of an arbitrary degree polynomial via brute force searching.

References

[1] Hadlock, C. R. (1978). *Field Theory and Its Classical Problems*. New York: MAA.

[2] Hardy, G. H., Wright, E. M., Heath-Brown, R. , Silverman, J. , Wiles, A. (2008). *An Introduction to the Theory of Numbers*, 6th ed. London: Oxford Univ. Press.

[3] Rudin, W. (1976). *Principles of Mathematical Analysis*, 3rd ed. New York: McGraw-Hill.