GALOIS THEORY

An introduction for (talented) beginners

Stephen McAdam
Deapartment of Mathematics
University of Texas at Austin
mcadam@math.utexas.edu

These notes are intended to be both a quick introduction to Galois Theory, as well as a training exercise for talented but not yet experienced students. I have assumed some basic exposure to abstract mathematics, but have tried to limit the amount needed. I do not assume familiarity with group theory, and very limited familiarity with beginning linear algebra. My basic goal was to write notes which I myself could have (propably) followed when I was a sophomore. (Admittedly, I was a smart sophomore, but no one ever came close to confusing me with a genius!) Athough the subject matter is more far reaching and sophisticated then appears in standard begining abstract mathematics texts, I have tried to keep the level of proof at about same level as such texts (used at good schools).

A few results are stated and used without proof. That was necessary to stay at the right level, and to adhere to the adjective "quick".

Many exercises are given, some easy, some less so. Some of them are later referred to as parts of a proof.

Due the the mysteries of software, occasionally a page number is missing. The math is all there.

Admittedly, these notes are neither fish nor fowl. They were originally conceived as a course for talented minority students attending a Summer math program at Berkeley. Truth in advertising forces me to admit that after writing them, I realized the six week long program was a few weeks too short to cover the material. As of this writing, these notes are untested. I hope that changes, and that someone will find them suitable for some setting (perhaps if not a standard class, then as some sort of honors work). In short, I hope these notes are neither too fishy nor too foul to be of use.

1 Introduction

If asked to solve the equation $X^2 = 2$, you would no doubt say the solution is $X = \pm\sqrt{2}$. This is correct, of course, for the very simple reason that the symbol $\sqrt{2}$ was defined to mean a (positive) number whose square is 2. That is to say, the symbol $\sqrt{2}$ was made up precisely to be the answer to our question. Of course the symbol i was defined to be a solution to the equation $X^2 = -1$, and so if you were asked to solve the equation $X^2 = -1$, you would say that the answer is $X = \pm i$. In exactly the same way, the symbol $\frac{3}{4}$ was made up to solve the equation $4X = 3$, and so if you were asked to solve the equation $4X = 3$, you would say the solution is $X = \frac{3}{4}$.

Suppose now that you were asked to solve $X^2 - 2X + \frac{1}{2} = 0$. You could proceed in the same fashion, and invent a symbol, let us say γ, such that γ is a solution to this equation. You would then say a solution is $X = \gamma$. However, it is not necessary to do that. We know by the quadratic formula that the solutions of $X^2 - 2X + \frac{1}{2} = 0$ are $X = 1 \pm \frac{\sqrt{2}}{2}$. We did not need to invent a new symbol. We could solve the problem using a symbol we had already invented, namely $\sqrt{2}$.

In general, the solution to

$aX^2 + bX + c = 0$ is $X = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. We did not need to invent a new symbol to do this, assuming that we already had the symbol $\sqrt{b^2 - 4ac}$.

What this amounts to is saying that by inventing enough symbols to solve $X^2 = d$ for any number d, we get for free (without anymore need to invent symbols) the solutions to any quadratic equation $aX^2 + bX + c = 0$.

What we will do in these notes is assume that we have enough symbols to solve $X^n = d$ for all positive integers n, and all numbers d, (i.e., we will asume we know what $\sqrt[n]{d}$ means), and then we will explore the question of what other polynomial equations $a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 = 0$ we can solve using these symbols, along with our standard operations of addition, subtraction, multiplication, and division.

Obviously, in this way we can solve any linear equation $aX + b = 0$, and the quadratic formula tells us how to solve any quadratic equation $aX^2 + bX + c = 0$. We shall shortly present a method of this sort allowing us to solve any cubic equation $aX^3 + bX^2 + cX + d = 0$. We also mention that there is a similar method to solve any quartic equation $aX^4 + bX^3 + CX^2 + dX + e = 0$, (but we will not present that method here).

The main bulk of our work, however, will be to show that there are some quintic polynomial equations which cannot be solved in this way. For instance, we will show that the equation $X^5 - 6X + 2$ cannot be solved in this manner.

Actually, in some philosophical sense, we cannot even find a solution of $X^2 = 2$. We already saw that saying the solution is $X = \pm\sqrt{2}$ begs the question, since we do not know what $\sqrt{2}$ is, other than it is a solution of $X^2 = 2$. A common way of "finding" $\sqrt{2}$, the way we use in pratical applications, is to approximate $\sqrt{2}$. Thus, we say that $\sqrt{2} \simeq 1.412$. We could, in fact, improve this approximation to any desired degree of accuracy. In that sense, we can find $\sqrt{2}$. In a similar way, we can find the solutions of $X^5 - 6X + 2$, by finding sufficiently good approximations to them.

(1.1) Exercise: Look up Newton's method (in almost any calculus book), and use it to find (i.e., approximate) the largest real root of $X^5 - 6X + 2$.

We stress that we are not saying that it is impossible to "find" a solution of $X^5 - 6X + 2 = 0$, only that a solution cannot be found by a particular method, namely restricting ourselves to doing additions,

subtractions, multiplications, divisions, and taking roots. (We will be more precise, later.)

Notation: We will use $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$ to denote the integrers, the rational numbers, the real numbers, and the complex numbers, respectively.

2 Cubic equations

In order to better appreciate the rigorous definition of what it means for a polynomial to be solvable by radicals, it will be helpful to look at the case of a cubic equation We will here present the method for solving any cubic equation. (We will simply present the method, without discussing the hard work that went into finding it.)

Starting with the cubic equation $aX^3 + bX^2 + cX + d = 0$, we may divide through by the leading coefficient a, and get an equation of the form $X^3 + pX^2 + qX + r = 0$. We first treat the special case in which $p = 0$. That is, we consider $X^3 + qX + r = 0$. We now show how to find the solutions of this equation. (By the way, those solutions are called the roots of $X^3 + qX + r$). The method is called Cardan's Formula. We blithely assume it was discovered by Cardan.

Let $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$. Let $\gamma = \sqrt{\frac{r^2}{4} + \frac{q^3}{27}}$. (In general, there are two choices for this square root. Pick either of

them.) Let $\alpha = \sqrt[3]{\frac{-r}{2} + \gamma}$. (In general, there are three choices for this cube root. Pick any one of them.) Let $\beta = \frac{-q}{3\alpha}$. Then the roots of $X^3 + qX + r$ are $\alpha + \beta$, $\alpha\omega + \beta\omega^2$, and $\alpha\omega^2 + \beta\omega$.

(2.1) Exercise: Show that $\alpha + \beta$, $\alpha\omega + \beta\omega^2$, and $\alpha\omega^2 + \beta\omega$ are the solutions of $X^3 + qX + r = 0$, by showing that $X^3 + qX + r = (X - (\alpha+\beta))(X - (\alpha\omega+\beta\omega^2))(X - (\alpha\omega^2+\beta\omega))$. (Hint: first, show that $\omega^2 + \omega + 1 = 0$, $\omega^3 = 1$, $\alpha\beta = -\frac{q}{3}$, and $\alpha^3 + \beta^3 = -r$.)

(2.2) Exercise: Find the roots of $X^3 + 3x + 2$.

We now turn to the general cubic equation $X^3 + pX^2 + qX + r = 0$. We will use a change of variable to reduce this problem to the special case we just discussed. Thus, we let $X = Y - \frac{p}{3}$. Substituting, we get $0 = X^3 + pX^2 + qX + r = Y^3 + (q - \frac{1}{3}p^2)Y + (r + \frac{2p^3}{27} - \frac{qp}{3}) = Y^3 + q'Y + r'$, with $q' = q - \frac{1}{3}p^2$, and $r' = r + \frac{2p^3}{27} - \frac{qp}{3}$. Since we know how to solve $Y^3 + q'Y + r' = 0$, we find the values of Y making this equation true, and then find the corresponding values of $X = Y - \frac{p}{3}$.

(2.3) Exercise: Find the roots of $X^3 + 6X^2 + 4X + 3$.

(2.4) Exercise: Find a change of variable which changes the polynomial $X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ into a polynomial of degree n whose X^{n-1} term has zero for its coefficient.

The Quadratic Formula was apparently discovered by Arabic mathematicians around 900 AD. The general cubic equation was probably first solved by Scipione del Ferro (1465-1526). The general quartic equation was solved by Ludovico Ferrari (1522-1565). (As we are not interested in solvable polynomials so much as unsolvable ones, we will not discuss Ferrari's work.) Inspired by these successes, mathematicians vigorously attacked the problem of trying to find the general solution of the quintic. It was not until the end of the eighteenth century that some people began to suspect that there was no such solution. Niels Abel (1802-1829) produced the first example of a nonsolvable quintic, and Evariste Galois (1811-1832) then perfected the theory of how to determine what polynomials are solvable.

3 Solvable by radicals

Vague Definition: A polynomial with rational coefficients is called solvable by radicals (over $\mathbf{Q}$) if its roots can be expressed using only rational numbers and succesive additions, subtractions, multiplications, divisions, and extractions of roots.

Remark: This definition is not really acceptable, since the phrase "can be expressed" is somewhat vague. For instance we can express the number e using only rational numbers and succesive additions, subtractions, multiplications, divisions, by saying e is the smallest (real) number bigger than $1 + 1 + \frac{1}{2} + \frac{1}{(2)(3)} + \cdots + \frac{1}{(2)(3)\ldots(n)}$ for all n. Yet this is not in the spirit of what we intended by a method of expression. We will now give a rigorous definition of what it means for a polynomial to be solvable by radicals over $\mathbf{Q}$.

Definition: Let $\alpha \in \mathbf{C}$. We say that α is obtainable by radicals over $\mathbf{Q}$ if there is a finite list of numbers $c_1, c_2, c_3, \ldots, c_m$, such that every number in this list is either in $\mathbf{Q}$, or is the sum, difference, product, or quotient of two earlier numbers in the list, or is an k-th root, for some positive integer k, of an earlier number in the list, and such that $c_m = \alpha$.

Definition: Let $f(X) \in \mathbf{Q}[X]$. We say that $f(X)$ is solvable by radicals over $\mathbf{Q}$ if every root of $f(X)$ is obtainable by radicals over $\mathbf{Q}$.

These definitions may seem a bit bizarre. Perhaps an example will make them less so.

Example: Using Cardan's Formula, we see that the roots of $X^3 - 6X + 4$ are $\alpha + \beta$, $\alpha\omega + \beta\omega^2$, and $\alpha\omega^2 + \beta\omega$, where

$$\alpha = \sqrt[3]{-2+2i}\,, \quad \beta = \frac{2}{\sqrt[3]{-2+2i}} = \frac{2}{\alpha}, \quad \text{and} \quad \omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}\,i.$$

We claim that each of these roots is obtainable by radicals over $\mathbf{Q}$ (so that $X^3 - 6X + 4$ is solvable by radicals over $\mathbf{Q}$). We will construct a list of numbers showing that $\alpha + \beta$ is obtainable by radicals over $\mathbf{Q}$, and leave the cases of the other two roots as an exercise. Since -1, -2, and 2 are in $\mathbf{Q}$, we may begin our list with them. Now since -1 is already part of our list, we may adjoin its square root, i, to the list. So far, we have -1, -2, 2, i. Since 2 and i are in our list, we may adjoin 2i, giving -1, -2, 2, i, 2i. Since -2 and 2i are in our list, we may adjoin -2+2i, giving -1, -2, 2, i, 2i, -2+2i. Since -2+2i is in our list, we may adjoin its cube root, giving

$-1, -2, 2, i, 2i, -2+2i, \sqrt[3]{-2+2i}$. Since this cube root is just α, we have $-1, -2, 2, i, 2i, -2+2i, \alpha$. Now 2 and α are in our list, and so we may adjoin the quotient $\frac{2}{\alpha} = \beta$. Thus our list becomes $-1, -2, 2, i, 2i, -2+2i, \alpha, \beta$. Finally, since α and β are in our list, we may adjoin the sum $\alpha + \beta$, giving $-1, -2, 2, i, 2i, -2+2i, \alpha, \beta, \alpha+\beta$. The existence of this list shows that $\alpha + \beta$ is obtainable by radicals over $\mathbf{Q}$.

(3.1) Exercise: Complete the demonstration that $X^3 - 6X + 4$ is solvable by radicals over $\mathbf{Q}$, by showing that its other two roots are obtainable by radicals over $\mathbf{Q}$.

Remark: Of course the list we found in this example is not the only possible list. For instance, we could have interchanged the first two terms, starting with $-2, -1$, instead of $-1, -2$. We could have thrown a 17 into the list anywhere except at the end. (It would not have helped, but it does not violate the rules.) Lots of variations are possible. All the definition requires is that there is at least one such list.

(3.2) Exercises: a) Show that $X^2 + 3X + 5$ is solvable over $\mathbf{Q}$.
b) Show that $X + 6$ is solvable over $\mathbf{Q}$.
c) Show that $X^3 + 6X^2 + 4X + 3$ is solvable over $\mathbf{Q}$.

Remark: The definition of what it means to say α is obtainable by radicals over $\mathbf{Q}$ requires that a certain type of list exist. It does not require that we actually know exactly what the list is. In the preceding example, we found a list. However, in general, actually finding the list is not required. It is enough that such a list exist, even if we do not know exactly what it is.

In the above example, we found the list by using Cardan's Formula. In general, we can see that when there is a formula (involving only rational numbers, sums, differences, products, quotients, and roots) giving the roots of the polynomial $f(X)$, then that formula will give us a way of actually finding the list which demonstrates that any root of $f(X)$ is obtainable by radicals over $\mathbf{Q}$. However, it is conceivable that some polynomial $f(X)$ is solvable by radicals, (i.e., the necessary lists exist), and yet there is no formula telling us how to find the roots of the polynomial It simply may happen that appropriate lists of numbers exist, but we do not know exactly how to find them.

We already mentioned that we will show that $X^5 - 6X + 2$ is not solvable by radicals over $\mathbf{Q}$. This will tell us that no formula just involving rational numbers, sums, differences, products, quotients, and roots, will give us all the roots of $X^5 - 6X + 2$. However, it tells us even more than that. It says that at least one of those roots simply cannot be part of a list

of the sort in the definition of being obtainable by radicals over $\mathbf{Q}$.

Remark: In the definition of α being obtainable by radicals over $\mathbf{Q}$, we are allowed to take roots, but not, for instance, sines. We could, if we wished, define a concept in which we are allowed to take sines but not roots. Thus, let us say that α is obtainable by sines over $\mathbf{Q}$ if there is a finite list of numbers $c_1, c_2, c_3, \ldots, c_m$, such that every number in this list is either in $\mathbf{Q}$, or is the sum, difference, product or quotient of two earlier numbers in the list, or is the tangent of an earlier number in the list, and such that $c_m = \alpha$.

(3.3) Exercise: Show that if α is obtainable by tangents over $\mathbf{Q}$, then $\alpha \in \mathbf{R}$.