Roots of Polynomials

http://personalpages.manchester.ac.uk/staff/goran.malic/roots_of_polynomials.pdf

1 Introduction

The study of the nature of polynomial roots was, and in some sense still is, one of the main driving forces for the development of mathematics, especially in the 18th and the 19th century. A large community of mathematicians, including many historical figures such as L. Euler, C.F. Gauss, J.R. Argand, N.H. Abel and E. Galois were concerned with answering the following two questions: how many roots does a polynomial have? Is there a formula which expresses the roots in terms of radicals?

What does it mean to have a formula which expresses the roots of polynomials in terms of radicals? Roughly put, a formula which expresses the roots of polynomials will be expressed in terms of radicals if only the operations of addition, subtraction, multiplication, division and taking the n-th root (and any combination of the aforementioned) are used in it. For example, roots of polynomials of degree 2, i.e. polynomials of the form $ax^2 + bx + c$, where $a \neq 0$, b and c are some complex numbers are expressed by the following formula:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

where the choice of a plus or a minus before the square root will give one of the two possible roots. This formula clearly is expressed in terms of radicals. However, the formula

$$x = \ln\left(e^{\frac{-b \pm \sqrt{b^2-4ac}}{2a}}\right),$$

is not expressed in terms of radicals (because the functions ln and e^x are present), even though it will calculate the roots correctly.

C.F. Gauss and J.R. Argand independently settled the question of the number of roots of a polynomial: a polynomial of degree $n \neq 0$ with complex numbers as coefficients has exactly n roots, counted with multiplicity. This result is known today as the Fundamental Theorem of Algebra.

The answer to the question of the existence of a formula that would express the roots of polynomials in terms of radicals was given independently by N.H. Abel, P. Ruffini and E. Galois. They proved that such a formula exists only for polynomials of degree 4 or less and that it is not possible to find such a formula for polynomials of degree 5 or larger. This result is known today as the Abel-Ruffini theorem. The methods that Galois used (or rather, invented) to prove the aforementioned theorem gave rise to a spectacular branch of mathematics called *Galois Theory*.

The goal of this project is to study the formulas for the roots of polynomials of degree between 1 and 4 and to informally discuss why such a formula does not exist for polynomials of degree 5 or larger. The project outline is as follows:

2 Project Outline

1. State the Fundamental Theorem of Algebra (in the form that states that polynomials with degree $n \neq 0$ have exactly n roots, counted with multiplicity) and give a brief account on the people involved with its proof. No more than 80 words is required for the second part.

2. Prove that for polynomials of degree 1 or 2 there exists a formula which expresses the roots in terms of radicals. Outline of the proof:

   - A general polynomial of degree 1 or 2 is of the form $ax + b$ or $ax^2 + bx + c$, respectively, where a, b and c are complex numbers and $a \neq 0$.
   - For polynomials of degree 1, what is the solution to $ax + b = 0$?
   - For polynomials of degree 2, prove that if x_0 is a root of $x^2 + \frac{b}{a}x + \frac{c}{a}$, then x_0 is a root of $ax^2 + bx + c$. Then simplify the following:

   $$\left(x - \frac{-b + \sqrt{b^2 - 4ac}}{2a}\right)\left(x - \frac{-b - \sqrt{b^2 - 4ac}}{2a}\right).$$

3. Discuss the formula for roots of polynomials of degree 3. Discussion outline:

   - Show that we only need to consider polynomials of the form $x^3 + px + q$. To do this first prove that if x_0 is a root of the polynomial $x^3 + \frac{b}{a}x^2 + \frac{c}{a}x + \frac{d}{a}$, then it is a root of the polynomial $ax^3 + bx^2 + cx + d$. Then show that any polynomial of the form $x^3 + ax^2 + bx + c$ can be reduced to a polynomial of the form $x^3 + px + q$, where $p = b - \frac{a^2}{3}$ and $q = \frac{2a^3}{27} - \frac{ab}{3} + c$ (hint: use the substitution $x = y - \frac{a}{3}$).
   - Show that the formula for the roots of a polynomial of the form $x^3 + px + q$ is given by

   $$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}.$$

   To show this let

   $$A = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} \text{ and } B = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}.$$

   Then calculate $A^3 + B^3$ and AB. Now simplify $x^3 = (A + B)^3$.

- Use the formula on the polynomial $x^3 + 6x - 2$. Verify that the number produced by the formula is indeed a root of the given polynomial.

4. Discuss the existence of a formula for roots of polynomials of degree 4 in the following way:

   - As before, show that we only need to consider polynomials of the form $x^4 + px^3 + qx^2 + rx + s$.
   - You can take the following as given: by using an appropriate, but rather messy substitution, a polynomial of the form $x^4 + ax^3 + bx^2 + cx + d$ can be reduced to a polynomial of the form $x^4 + px^2 + qx + r$. Surprisingly, we can also get rid of the x^4 and reduce the polynomial $x^4 + px^2 + qx + r$ to the polynomial $x^3 - 2px^2 + (p^2 - 4r)x + q^2$. Now we can use the formula for the roots of polynomials of degree 3 to find the three roots x_1, x_2 and x_3 of the polynomial $x^3 - 2px^2 + (p^2 - 4r)x + q^2$. Four of the eight numbers

$$\frac{\sqrt{x_1}+\sqrt{x_2}+\sqrt{x_3}}{2}, \quad \frac{\sqrt{x_1}+\sqrt{x_2}-\sqrt{x_3}}{2}, \quad \frac{\sqrt{x_1}-\sqrt{x_2}+\sqrt{x_3}}{2}, \quad \frac{\sqrt{x_1}-\sqrt{x_2}-\sqrt{x_3}}{2},$$
$$\frac{-\sqrt{x_1}+\sqrt{x_2}+\sqrt{x_3}}{2}, \quad \frac{-\sqrt{x_1}+\sqrt{x_2}-\sqrt{x_3}}{2}, \quad \frac{-\sqrt{x_1}-\sqrt{x_2}+\sqrt{x_3}}{2}, \quad \frac{-\sqrt{x_1}-\sqrt{x_2}-\sqrt{x_3}}{2}$$

     will be the roots of the polynomial $x^4 + px^2 + qx + r$.
   - Reduce the polynomial $x^4 + 4x + 3$ to a cubic polynomial and find the four roots of $x^4 + 4x + 3$ (here $p = 0$, $q = 4$ and $r = 3$).

5. We informally discuss why is there no formula which would express roots of polynomials of degree 5 or larger in terms of radicals. We will consider the polynomial $x^5 - x + a$, where a is some complex number.

   - It is important to realize that if we show that there is no such formula for just one polynomial of degree 5, then there is no such formula *in general*. To have such a formula in general means that it must be valid for *all* polynomials of degree 5. Hence, if it is not valid for just one polynomial of degree 5, then it is not valid in general.
   - You could say the following: OK, I accept that there is no such formula for polynomials of degree 5. However, what about polynomials of degree 6 or 17? Or for that matter, any polynomial of degree $n > 5$? To answer this, we notice that if there is such a formula for the roots of $x^5 - x + a$, then there is no formula for the roots of $x^n - x^{n-4} + ax^{n-5}$, for $n \geq 5$ since

$$x^n - x^{n-4} + ax^{n-5} = x^{n-5}(x^5 - x + a).$$

     Hence the roots of $x^n - x^{n-4} + ax^{n-5}$ are the roots of $x^5 - x + a$ and 0. Therefore, if we show that there is no such formula for the polynomial $x^5 - x + a$, then we can immediately find a polynomial of degree $n > 5$ for which there is no formula in terms of radicals.

- By the Fundamental Theorem of Algebra, the polynomial $x^5 - x + a$ has five roots, counted with multiplicity. We will be interested only in those values a for which $x^5 - x + a$ has five distinct roots, i.e. five roots with multiplicity 1.
- We claim that $x^5 - x + a$ has five distinct roots if a is not equal to $\pm\frac{4}{5\sqrt[4]{5}}$ or $\pm\frac{4i}{5\sqrt[4]{5}}$. In other words, a^4 must not be equal to $\frac{4^4}{5^4}$. To show this, argue as follows:
  - Suppose that b is a root of $x^5 - x + a$ with multiplicity 2 or larger. Then $x^5 - x + a = (x - b)^2 p(x)$, where $p(x)$ is some polynomial of degree 5 (note that $p(x)$ may also have $(x - b)$ as a factor, as b can be a root of multiplicity 3, 4 or 5, but that does not concern us). Substitute $x = b+\varepsilon$ for x in $x^5 - x + a$ and verify that

    $$5b^4 - 1 = \varepsilon \cdot (p(b + \varepsilon) - 10b^3 - 10b^2\varepsilon - 5b\varepsilon^2 - \varepsilon^3).$$

    (Don't forget to use $b^5 - b + a = 0$ as b is a root!).
  - We consider the number ε to be an arbitrarily small, but still a positive number. We have found that

    $$5b^4 - 1 = \varepsilon \cdot \alpha \text{ where } \alpha = p(b + \varepsilon) - 10b^3 - 10b^2\varepsilon - 5b\varepsilon^2 - \varepsilon^3,$$

    and the formula $5b^4 - 1 = \varepsilon \cdot \alpha$ is valid for any choice of ε. Therefore, we can choose a very small ε, for example, $\varepsilon = 0.00001$ and conclude that $5b^4 - 1 = 0.00001 \cdot \alpha$. By choosing a smaller and smaller ε, the value of $5b^4 - 1$ gets smaller and smaller. Hence, by repeatedly choosing a smaller and smaller ε (imagine it as a number $0.0\ldots01$ with so many zeros after the decimal point that it is for all reasons and purposes indistinguishable from 0), the value of $5b^4 - 1$ will be indistinguishable from 0. Therefore, $5b^4 - 1 = 0$.
  - We have concluded that if b is a root of $x^5 - x + a$ with multiplicity at least 2, then $5b^4 = 1$. Show that $a^4 = \frac{4^4}{5^4}$ (hint: use $b^5 - b + a = 0$, i.e. $a = b - b^5$ and raise to the fourth power).
- Now we inspect how the roots of $x^5 - x + a$ behave when we vary a but in a specific way: we start with $a = 0$. Our polynomial is now $x^5 - x$ and its five roots are $0, 1, i, -1$ and $-i$. Then we continuously move a along the x-axis towards $\frac{4}{5\sqrt[4]{5}}$. Just before we reach $\frac{4}{5\sqrt[4]{5}}$, instead of crushing into it (remember, we're not interested in $a = \frac{4}{5\sqrt[4]{5}}$ because then $x^5 - x + a$ has a root with multiplicity at least 2) we circle around it in a counter-clockwise fashion until we make a full circle and we're back on the x-axis. Then we continuously move back towards 0. In other words, our parameter a traces out a loop starting at 0 and going around $\frac{4}{5\sqrt[4]{5}}$ once in a counter-clockwise fashion.
- For a visualization of the variation of a, please visit: `personalpages.manchester.ac.uk/staff/goran.malic/a.gif`

- As a varies, so do the five roots of $x^5 - x + a$. For a visualization of the variation of the roots of $x^5 - x + a$ as a varies, please visit: personalpages.manchester.ac.uk/staff/goran.malic/f1.gif
- We notice the following: the roots whose starting points are at $i, -1$ and $-i$ (brown, purple and red curves, respectively) also finish their journey at their respective starting points. However, the root with starting point 0 (light blue) finishes at point 1 and the root with starting point 1 (dark blue) finishes at the point 0.
- An appropriate way of writing down this information is by using *permutations of a set*.
  - A permutation of a finite set A is a map $f\colon A \to A$ with the following property: for every two distinct elements $a, b \in A$, the images $f(a)$ and $f(b)$ are also distinct.
  - We often take A to be the set $\{1, 2, \dots, n\}$ of the first n positive integers. Let us look at some examples: if $A = \{1, 2\}$, then the two possible permutations of A are the maps $f(1) = 1, f(2) = 2$ and $g(1) = 2$, $g(2) = 1$. If $A = \{1, 2, 3\}$, one permutation of A is $f(1) = 3$, $f(2) = 1$ and $f(3) = 2$. A useful form for writing permutations is the following:

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

    and we interpret it in the following way: the top row represents the elements of the set $A = \{1, 2, 3\}$. The bottom row represents the images $f(1)$, $f(2)$ and $f(3)$, in that order. Since we chose a permutation in which $f(1) = 3$, $f(2) = 1$ and $f(3) = 2$, the bottom row must read $3 \quad 1 \quad 2$.
  - Write all permutations of $A = \{1, 2, 3\}$ in the previously described form. There are 6 of them.
  - Two permutations f and g can be multiplied as follows: let

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \text{ and } g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

    The product fg will be of the form

$$fg = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ fg(1) & fg(2) & fg(3) \end{pmatrix}.$$

    To calculate $fg(1)$, we first look at $g(1)$. We have $g(1) = 2$. Then $fg(1) = f(2) = 1$. Then we look at $g(2)$ and find that $g(2) = 1$, hence $fg(2) = f(1) = 3$. We are left with $g(3) = 3$, hence $fg(3) = f(3) = 2$. Therefore,

$$fg = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

- Note that the product of permutations f and g, when viewed as functions $f(x)$ and $g(x)$, represents the composition function $f(g(x))$.
- Choose any 3 permutations f, g, h of the set $\{1, 2, 3\}$ and calculate the products fg, gf, fh, hf, gh and hg. Note that fg will almost never be the same as gf!

- Let us label the roots $0, 1, i, -1$ and $-i$ of $x^5 - x + 0$, with 1,2,3,4 and 5, respectively. After the parameter a finishes with traversing the loop around $\frac{4}{5\sqrt[4]{5}}$, the roots with labels 3,4 and 5 will return to their original positions, but the roots with labels 1 and 2 will switch places, i.e. the root with label 1 will end up at the starting position of the root with label 2 and vice-versa. We can write this information as the following permutation:

$$f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}.$$

- Now suppose that the parameter a traverses a loop around $\frac{4i}{5\sqrt[4]{5}}$ by starting at 0 and moving towards $\frac{4i}{5\sqrt[4]{5}}$ along the positive part of the imaginary axis, and as before, just as a is about to crash into $\frac{4i}{5\sqrt[4]{5}}$ it starts circling around $\frac{4i}{5\sqrt[4]{5}}$ in a counter-clockwise fashion, and returns to 0 along the imaginary axis after it completes a full circle around $\frac{4i}{5\sqrt[4]{5}}$. In this case, the trajectories of the roots of $x^5 - x + a$ will be rotated by 90 degrees relative to the trajectories in the previous case. If we keep the same labels on our roots $0, 1, i, -1$ and $-i$ of $x^5 - x$, then we find that the roots with labels 2, 4 and 5 have returned to their original positions but the roots with labels 1 and 3 have switched places. We write this information as the following permutation:

$$f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}.$$

- For a visualization, visit:
`personalpages.manchester.ac.uk/staff/goran.malic/f2.gif`
- Similarly, if a traverses a loop around $-\frac{4}{5\sqrt[4]{5}}$ by starting at 0, or a loop around $-\frac{4i}{5\sqrt[4]{5}}$ by starting at 0, the roots will change their positions in the following two ways:

$$f_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix} \text{ and } f_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix}.$$

- For a visualization, please visit:
`personalpages.manchester.ac.uk/staff/goran.malic/f3.gif`
`personalpages.manchester.ac.uk/staff/goran.malic/f4.gif`
- All possible permutations of the set $\{1, 2, 3, 4, 5\}$ can be realized as a product of the permutations f_1, f_2, f_3 and f_4. The proof of this fact uses a rather

tiresome argument so for now you will have to take my word for it. You can experiment by first choosing a random permutation of the set $\{1,2,3,4,5\}$, and then finding a product of the permutations f_1, f_2, f_3 and f_4 which will give the same permutation.

- There are 120 permutations of the set $\{1,2,3,4,5\}$. To show this, argue as follows: a permutation f of the set $\{1,2,3,4,5\}$ can map 1 into any element of the set $\{1,2,3,4,5\}$. Therefore, there are 5 choices for the value of $f(1)$. Using the fact that a permutations must map distinct elements of $\{1,2,3,4,5\}$ to distinct images, conclude that there are only 4 choices for the value of $f(2)$ (hint: $f(2)$ can take any value in $\{1,2,3,4,5\}$ which is not equal to $f(1)$). Similarly conclude that after choosing the values of $f(1)$ and $f(2)$, there are only 3 choices for the value of $f(3)$. Next, conclude that after choosing the values of $f(1), f(2)$ and $f(3)$, there are only 2 choices for the value of $f(4)$ and finally, conclude that after choosing the values of $f(1), f(2), f(3)$ and $f(4)$, there is a single choice for the value of $f(5)$. Therefore, the total number of permutations is $5\cdot 4\cdot 3\cdot 2\cdot 1 = 120$.
- Calculate $g_1 = f_1f_2f_3f_4$, $g_2 = f_4f_3f_2f_1$ and g_1g_2.
- We have now concluded that the roots of the polynomial $x^5 - x + a$, as a varies along the loops starting at 0 and going around $\pm\frac{4}{5\sqrt[4]{5}}$ or $\pm\frac{4i}{5\sqrt[4]{5}}$ once in a counter-clockwise fashion give rise to 120 permutations. By a rather sophisticated argument given by E.Galois, a formula in terms of radicals that would produce the roots of a polynomial can exist only if the roots of a polynomial give rise to no more than 24 permutations.

3 Literature

Your main reference should be lectures 4 and 5 from:

D. Fuchs, S. Tabachnikov. *Mathematical Omnibus: Thirty Lectures on Classic Mathematics*, Providence, RI, American Mathematical Society 2007.

This text is freely available on-line at `www.math.psu.edu/tabachni/Books/taba.pdf` and it covers the topic of the project in sufficient detail. The text also includes a full proof of the non-existence of a formula for roots of polynomials of degree 5 or larger, if you find the explanation outlined in the project unsatisfactory.

You should also consult the standard textbooks for your math course to learn about some elementary properties of polynomials and complex numbers. A textbook that covers elementary properties of permutations could also be of use.

4 Prerequisites

Knowledge of elementary facts about polynomials: the degree of a polynomial, general form for a polynomial of arbitrary degree, roots of a polynomial. Elementary facts about complex numbers: the motivation behind introducing the imaginary unit $i = \sqrt{-1}$ as a root of the polynomial $x^2 + 1$. The real and the imaginary part of a complex number. Placement of complex numbers in the plane.