Cubic, Quartic, and Quintic Equations

C. Godsalve
email:seagods@hotmail.com

July 13, 2009

Contents

1 Introduction

This article is intended to be *highly informal* and non rigourous. Its audience might be readers who are curious about these topics, but are either not ready for a rigourous approach, or just want to get a "flavour" of the study of polynomials. We hope to whet the reader's appetite to go on to more formal texts, or if not, to have gained at least a vague impression of the most basic parts of the underlying mathematics. Nothing is proved here, however the author may extend and revise this article in the future.

Now, the quadratic equation is studied at GCSE level (normally taken by 16 year olds in the UK) but the cubic is not. The cubic equation is in fact a *much* more difficult problem to solve. It is not even part of the A-level syllabus (university entrance in the UK), though a good A-level student should be able to follow this article.

First, we include a small revision section on complex numbers, including polar form, and complex numbers as exponentials with imaginary arguments.

The first sections on cubics and quartics use what might be called "by hook or by crook" methods. These methods were devised in Italy during the Renaissance. After this we revisit the quadratic, cubic, and quartic equations from a completely different point of view.

To do this, we introduce the Discrete Fourier transform (DFT). The reader may not have heard of the DFT before, however, the brief revision of complex numbers should make it easily intelligible. This DFT enables us to re-examine quadratic, cubic, and quartic equations, and treat them all in exactly the same unified manner. In doing this we encounter groups and very basic group theory. Although the introduction of groups is cursory, the reader will see why group theory grew out of the study of polynomial equations.

At the end we take a brief look at the quintic equation, and why *in general* it is not solvable in terms of *radicals*. The term radical just means things involving $\sqrt{}$, $\sqrt[3]{}$, and so on (it comes from the word radix, and $\sqrt{}$ seems to be an old German way of writing r). We then explain what that insolubility does and doesn't mean.

At the end, we give a brief practical note on how we can always find the roots of any polynomial of any order by numerical means. Finally, we give a very brief historical sketch of the subject.

2 Complex Numbers

In this small section, we give a brief revision of complex numbers, and introduce the fundamental theorem of algebra. Many readers may just skip this section altogether. However, some notation and caveats are introduced, so it may be worth a quick "scan" even if the reader is needs no revision.

There is no such number on the real number line that, when squared, gives you a negative number. So $(-3) \times (-3)$ gives you 9, just as 3×3. Conversely, that means that there is no such number which is the square root of a negative number on the real number line. So, if your solution to a quadratic has a positive argument for the square root, we have two places where the parabola cuts the x axis. If the square root has argument zero, the parabola just touches the line, but if the argument is negative, the parabola just doesn't cut the x axis anywhere. It's either all above, or all below the x axis.

Suppose we *define* a new kind of number called an *imaginary number* that, when squared gives a negative real number. You can define all kinds of things in mathematics, as long as you stick to logic once you have defined everything properly, it all makes mathematical sense. Not many definitions made by just a whim, as it were, turn out to be useful. But the definition of imaginary numbers (and later complex numbers) turn out to be very useful. This is why engineers have to learn about them for instance.

So, we define the unit imaginary number i to be $i = \sqrt{-1}$. Now, the the square root of two numbers a and b multiplied together is $\sqrt{ab} = \sqrt{a}\sqrt{b}$, so $\sqrt{(-1) \times 5} = \sqrt{-1}\sqrt{5}$. That is $\sqrt{-5} = \sqrt{5} \times i$. In defining i this way, we have the square roots of all negative numbers in terms of the square root of the positive number times i.

Now we have the unit imaginary number, we can go straight onto to *complex* numbers. That is a *complex* of a real and an imaginary number. By this, we mean a sum of a real number and an imaginary number. The number $6i$ is imaginary, because if it is squared it gives -36 (as does the square of $-6i$). So, the number $(5 + 6i)$ is a complex number. If a and b are real numbers, then the number $Z = a + bi$ is a complex number. Complex numbers can be multiplied out as brackets. For instance, if c and d are real numbers as well, then

$$(a + bi) \times (c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i. \tag{1}$$

Given a complex number $Z = a + bi$, there is another complex number called its *complex conjugate*. It is denoted as $Z^* = a - bi$. It is useful because of the difference of two squares. You can verify that

$$Z \times Z^* = Z = a^2 + b^2. \tag{2}$$

So, a complex number, multiplied by its complex conjugate, always gives you a real number. A useful manipulation to spot is

$$\frac{1}{a + bi} = \frac{1}{a + bi} \times \frac{a - bi}{a - bi} = \frac{a - bi}{a^2 + b^2}. \tag{3}$$

This means we can change any complex denominator in a fraction into a real one. Of course, it follows that $1/i = -i$.

Now, suppose we solved a quadratic equation, and found two roots r and s. Then we

can write the quadratic down as

$$(x - r)(x - s) = 0. \tag{4}$$

Clearly, if we expand the brackets we have a quadratic equation

$$x^2 - (r + s)x + rs = 0. \tag{5}$$

Obviously if s and r are real, there is no problem. But what if s is a complex number? This might be expected if the coefficients were complex, but we suppose we were given a quadratic equation with all real coefficients. Then that means $r + s$ must be real, as must rs. *If one root is complex, another root must be its complex conjugate.* That is the roots of a polynomial must be either real, or occur in complex conjugate pairs.

This takes us to the *fundamental theorem of algebra* which we shall only state. One way of putting it is that for any polynomial equation of degree n,

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 = 0, \tag{6}$$

there are *always* exactly n roots to the polynomial. Here, and in the following sections, we suppose that the as are all *real* coefficients. We make two remarks: we insist that $a_n \neq 0$, also we insist that $a_0 \neq 0$. If a_n were zero, we would have a polynomial of degree $n - 1$ (or less). If $a_0 = 0$, then we have x times a polynomial of degree $n - 1$. In fact, we shall *always* divide by a_n so the coefficient of x^n will automatically be one.

So, for the quadratic equation, the degree n is just 2. Following the same reasoning as above, if *any* complex root is found, then one other root is its complex conjugate. Otherwise, when we write down the polynomial in terms of its roots, we would find that we have complex coefficients, but the coefficients are known to be real.

So, what about the cubic equation $x^3 = 1$? This is of degree three, with $a_3 = 1$, $a_2 = a_1 = 0$, and $a_0 = -1$. Clearly, the number one is a solution because $1 \times 1 \times 1 = 1$. It is easy to check out that

$$\left(-\frac{1}{2} \pm \frac{\sqrt{3}}{2} i\right)^3 = 1, \tag{7}$$

so these two numbers along with 1 are the three cube roots of one.

Complex numbers can be written in what is called *polar form*. Any complex number Z can be written as $\rho\,(\cos\phi + i\,\sin\phi)$ where both ρ and ϕ are real. Now, if we raise this complex number to a power, then

$$[\rho\,(\cos\phi + i\,\sin\phi)]^n = \rho^n\,(\cos(n\phi) + i\,\sin(n\phi))\,. \tag{8}$$

For readers who are familiar with the McLaurin expansions for e^x, $\cos x$, and $\sin x$, check out that

$$e^{i\phi} = \cos\phi + i\sin\phi \tag{9}$$

which is why eqn.8 works.

3 Cubic Equations

The story of the general algebraic solution of the cubic equations goes back to renaissance Italy. Back then, you could stand up in the University lecture hall and challenge the mathematics professor for his job! You would wave about a piece of paper with a list of problems on it that you had solved, but that you didn't think the professor could solve. The professor would give you problems that he didn't think you could solve, and a mathematical duel would begin. The audience would decide the winner. It was a time of great secrecy in mathematics for this reason. Careless talk meant that you no longer had the edge, and your days as professor were numbered.

The quadratic was solved in ancient times, but it took until 1541 for the general case of the cubic to be solved. Clearly, the cubic equation is a much tougher proposition than the quadratic equation.

Here is the general cubic equation

$$x^3 + ax^2 + bx + c = 0. \tag{10}$$

We have already divided through by any coefficient that x^3 may have had. Now we use the trick of the linear shift. That is we replace x with $x + S$ where S is an arbitrary number. Then

$$x^3 + 3Sx^2 + 3S^2x + S^3 + a(x^2 + 2Sx + S^2) + b(x + S) + c = 0. \tag{11}$$

Now the trick is to give S a value that makes the coefficient of x^2 disappear, that is we choose S so that $(3S + a) = 0$. So we are now solving

$$x^3 + Ax + B = 0. \tag{12}$$

This cubic, without an x^2 term is called a *depressed cubic*. Here A and B are numbers that depend on a, b, c. If we can solve this, we can then get the roots of the original equation by shifting back.

We shall look at two methods to solve the cubic, both of which are equivalent. We shall proceed by an example. We are to solve

$$x^3 - 10x^2 + 31x - 30 = 0. \tag{13}$$

We can work out that if we put $x \to x - 10/3$, then

$$x^3 - \frac{21}{9}x - \frac{20}{27} = 0. \tag{14}$$

We have converted the original problem into a depressed cubic.

There are two ways of solving this depressed cubic, the first looks bit crazy at first, but is entirely equivalent to the second given here.

3.1 First Method

.

The idea of the first method is, that we can find a solution that is going to be a difference between the cube roots of two numbers U and V. That is to say, one root is at $x = \sqrt[3]{U} - \sqrt[3]{V}$. Then substituting this x into eqn.24 gives us

$$U - 3\sqrt[3]{U}\sqrt[3]{V}\left(\sqrt[3]{U} - \sqrt[3]{V}\right) - V - \frac{21}{9}(\sqrt[3]{U} - \sqrt[3]{V}) - \frac{20}{27} = 0,$$

or

$$U - V - \frac{20}{27} + (\sqrt[3]{U} - \sqrt[3]{V})\left(-3\sqrt[3]{U}\sqrt[3]{V} - \frac{21}{9}\right) = 0. \tag{15}$$

Now, we obviously have *one* solution if by any chance there happens to be a U and a V such that

$$U - V - \frac{20}{27} = 0, \tag{16}$$

and

$$-3\sqrt[3]{U}\sqrt[3]{V} - \frac{21}{9} = 0. \tag{17}$$

The last bit can be written

$$UV = -\left(\frac{21}{27}\right)^3. \tag{18}$$

So, if we multiply eqn.16 by U and use eqn.18, we get

$$U^2 - \frac{20}{27}U + \left(\frac{21}{27}\right)^3 = 0. \tag{19}$$

Now we see that whatever the coefficients are, we always get a $U - V = something$ equation and a $UV = something$ equation. Desperate as it seemed at first, we can always get a quadratic, and so we are well on the way to finding one root.

So, we have it! We have a quadratic for U, and we can get another quadratic for V. Then we have one solution. If it is complex, we already have another. If we have a real root we can factor it out of the depressed cubic to get another quadratic. If we have a complex conjugate pair, we can factor their product out of the depressed cubic and get the third root.

We won't leave it there though. It is instructive to look at the details here. The solution to the quadratic is

$$\begin{aligned} 2U &= \frac{20}{27} \pm \sqrt{\left(\frac{20}{27}\right)^2 - 4\left(\frac{21}{27}\right)^3} \\ &\frac{20}{27} \pm \frac{2}{27}\sqrt{100 - 21^3/27} \\ &= \frac{20}{27} \pm \frac{2}{27}\sqrt{-243}. \end{aligned} \tag{20}$$

We note that 243/27=9 and that $\sqrt{27} = 3\sqrt{3}$ so that

$$U = \frac{10}{27} \pm \frac{i}{\sqrt{3}}. \tag{21}$$

Now what we actually want is the cube root of U. Let's start off by expressing U in polar form.

$$U = \rho(\cos\phi + \sin\phi) \tag{22}$$

where

$$\begin{aligned}\rho &= \sqrt{\left(\frac{10}{27}\right)^2 + \frac{1}{3}} \\ &= \sqrt{\left(\frac{10}{27}\right)^2 + \frac{1\times 9\times 27}{3\times 9\times 27}} \\ &= \sqrt{\frac{100+243}{27^2}}.\end{aligned} \tag{23}$$

Now $343 = 7^3$ and $27^2 = 9^3$ so we have a "nice" value for $\sqrt[3]{\rho}$.

$$\rho = \sqrt{\sqrt{\sqrt{\left(\frac{7^3}{9^3}\right)}}} = \sqrt{\sqrt[3]{\left(\frac{7^3}{9^3}\right)}} = \frac{\sqrt{7}}{3}. \tag{24}$$

The angle ϕ is just given by

$$\phi = \arctan\left(\frac{10}{27\sqrt{3}}\right). \tag{25}$$

A similar quadratic can be found for V, and it turns out that

$$V = -\frac{10}{27} \pm i\sqrt{3} \tag{26}$$

and so we have

$$\sqrt[3]{U} = \sqrt[3]{\rho}\left(\cos\frac{\phi}{3} + i\sin\frac{\phi}{3}\right), \tag{27}$$

and

$$\sqrt[3]{V} = -\sqrt[3]{\rho}\left(\cos\frac{\phi}{3} - i\sin\frac{\phi}{3}\right). \tag{28}$$

At last we can take the difference of the two cube roots, that is

$$\sqrt[3]{U} - \sqrt[3]{V} = 2\sqrt{\frac{7}{9}}\cos\frac{\phi}{3} = \frac{5}{3}. \tag{29}$$

It is needless to say we have set up the coefficients so that we get tidy numbers here. Let's press on. We have one root, so we know that there are two numbers A and B such that

$$\left(x - \frac{5}{3}\right)(x^2 + Ax + B) = x^3 - \frac{21}{9}x - \frac{20}{27} = 0. \tag{30}$$

So, A and B are 5/3 and 4/9. The roots of the quadratic are -1/3 and -4/3. Of course after all this we have to remember these are the roots of the depressed cubic. We have to reverse the shift we made to get the roots of the cubic we wanted to solve. Once this is done we have the roots of the original cubic, which are 2, 3, and 5.

3.2 Second Method

The second method is to introduce some arbitrary parameter s into the equation and then fix this parameter to be a particular value to make the "nasty bits" disappear. It might sound dodgy, but let's have a look. Suppose we make the transformation

$$x \to z + \frac{s}{z}. \tag{31}$$

If we substitute this into our depressed cubic (the one in the last section) we get

$$z^3 + 3\frac{s}{z} + 3\frac{s^2}{z} + \frac{s^3}{z^3} - \frac{21}{9}\left(z + \frac{s}{z}\right) - \frac{20}{27}. \tag{32}$$

Gathering terms we get

$$z^3 + z\left(3s - \frac{21}{9}\right) + \frac{s}{z}\left(3s - \frac{21}{9}\right) + \frac{s^3}{z^3} - \frac{20}{27}. \tag{33}$$

Now, we can choose s to be $21/27$, so that both terms in parentheses vanish. Putting $U = z^3$ gives

$$U + \left(\frac{21}{27}\right)^3 \frac{1}{U} - \frac{20}{27}. \tag{34}$$

Looks kind of familiar doesn't it?

4 Quartic Equations

Not long after the general cubic equation was solved, the general quartic was solved too. The first step is to do a linear shift, as we did with the cubic. This linear shift gives us the depressed quartic where the coefficient of x^3 is zero. We won't bother with the details of that, but suppose we have already done it, and write down the quartic

$$x^4 + ax^2 + bx + c = 0. \tag{35}$$

Now we make a seemingly pointless observation that

$$(x^2 + a)^2 = x^4 + 2ax^2 + a^2. \tag{36}$$

Because of this we can write our depressed quartic as

$$(x^2 + a)^2 - 2ax^2 - a^2 + ax^2 + bx + c = 0$$

or

$$(x^2 + a)^2 = ax^2 + a^2 - bx - c. \tag{37}$$

There is of course, the possibility that the right hand side could be a perfect square, but this is unlikely. If it were though, we could just square root both sides and get two roots

from the quadratic. Recall in the last section, we introduced an arbitrary parameter s and fixed it later. We so do something similar here. We can write

$$(x^2 + a + s)^2 = x^4 + 2ax^2 + 2sx^2 + a^2 + 2as + s^2$$
$$= (x^2 + a)^2 + 2sx^2 + 2as + s^2$$

or

$$(x^2 + a)^2 = (x^2 + a + s)^2 - 2sx^2 - 2as - s^2. \tag{38}$$

If we substitute this we get

$$(x^2 + a + s)^2 = ax^2 + a^2 + 2sx^2 + 2as + s^2 - bx - c. \tag{39}$$

So, this will hold true for any value of s. The trick now, is to cast the right hand side as $Ax^2 + Bx + C$. If we can find an s such that $\sqrt{B^2 - 4AC} = 0$, then the right hand side is a perfect square! It turns out we can always do this. We will always find that s is the root of a cubic, and we can find the roots of those.

5 The Discrete Fourier Transform, Roots, and Groups

Many readers will have been introduced to the Discrete Fourier Transform (DFT) in data analysis. It is often used to give a spectral analysis of evenly spaced data. It may seem surprising that the DFT has anything to so with polynomials.

I shall suppose the reader has never heard of the discrete Fourier transform before. However, armed with our short section on complex numbers, everything should become clear. There is some notation that may be unfamiliar.

First we shall use subscripts, so instead of calling the three roots of a cubic (for instance) r, s, and t we call them r_0, r_1, and r_2. The quantity "r one squared" looks like r_1^2. Also, $\sum$ stands for "sum over". So

$$S = \sum_{i=0}^{i=2} a_i x^i \tag{40}$$

just means that $S = a_0x^0 + a_1x^1 + a_2x^2 = a_0 + a_1x + a_2x^2$.

From our current point of view, the discrete Fourier transform maps a given a set of complex numbers r_k, to another set of complex numbers s_k. We use the notation r_k because these r_k are going to represent the roots of a polynomial. The numbers s_k are given by

$$s_k = \sum_{n=0}^{N-1} r_k e^{-2\pi ikn/N},\ k = 0,\ 1,\ \ldots,\ N-1. \tag{41}$$

Note that the N numbers which are the Nth root of 1 are given by $e^{2\pi in/N}$ where $n = 0, 1, 2, 3, \ldots N-1$. We state without proof that the inverse transform happens to be

$$r_k = \frac{1}{N} \sum_{n=0}^{N-1} s_k e^{2\pi ikn/N}. \tag{42}$$

Now, we have intimated that the r_k are to be the roots of our polynomial. If we write down our polynomial in terms of the unknown roots, it looks like

$$(x - r_0)(x - r_1)(x - r_2) \dots (x - r_{N-1}). \tag{43}$$

The expansion for a cubic, for instance is then

$$x^3 - (r_0 + r_1 + r_2)x^2 + (r_0 r_1 + r_1 r_2 + r_2 r_0)x - r_0 r_1 r_2. \tag{44}$$

Note that we can put $r_0 \to r_1$, $r_1 \to r_0$ and absolutely nothing is changed. The roots form a finite *symmetry group* and the coefficients are *symmetric* under permutations of the group elements r_i. Note also, that the terms are *homogeneous* of degree three. For instance $r_0 r_1 x = r_0^1 r_1^1 x^1$, if we add the indices we get 1+1+1=3 so it is of degree three. So $r_1^1 x^2$ is also of degree three, and so on. By homogeneous, we mean that all the terms have the same degree.

We shall only state the bare minimum about groups for the purposes of this article. A symmetry group is a set of objects, with an operator defined on those objects which leaves something unchanged. In this case the operator swaps pairs of roots. It is a symmetry group because a swap leaves things (the coefficients of the polynomial) unchanged. There *must* be an inverse for every operation, *and an identity operator*, otherwise the set of objects and the operation do not form a group. The inverse here is to do the same swap, and the identity is just "make no swap".

Often the idea of a symmetry group is introduced using shapes. For instance we might have as our objects the three corners of an equilateral triangle. The triangle is unchanged by a rotation through 120° for instance. Introducing groups in this way often seems odd to students, but the three cube roots of unity form an equilateral triangle in the complex plane, and multiplication by $e^{2\pi i/3}$ is equivalent to a rotation through 120° and leaves the triangle unchanged. There is a direct connection between shapes and the roots of unity. We shall come across another type of group later.

We have a finite set of numbers (the roots), and we know that all the coefficients of the polynomial are functions of the roots, and these coefficients are all unchanged if we swap any pair of roots. Absolutely *any* permutation of the roots can be achieved by simple pair swaps. Note that if we permute any permutation of a set of objects we just have another permutation of the set of objects. A permuation of (abc) cannot give (adc). This property is called *closure*. If set of objects is defined with an operation that does not have closure, it is not a group.

Note the similarity between the discrete Fourier transform and the inverse. Suppose r_i, $i = 0,\ 1,\ 2.$ are the roots of a cubic. We might suspect from this similarity in the relations in the discrete Fourier transform and the inverse, that the s_i are *also* the roots of *another but different* cubic equation.

This new cubic may might not be in s, it might be in in s^3 for instance. That is the s_i might be the roots of $(s^3 - s_0^3)(s^3 - s_1^3)(s^3 - s_2^3) = 0$. Note that s_0 is always the sum of the roots, which is always the coefficient of x^{n-1} if the degree of the polynomial is n. That is to say we *always have* the value of s_0 immediately. The other s_i are the roots of a polynomial of degree $n-1$. So, *if* we can find the coefficients of this polynomial then we can solve the polynomial of lower degree. Once we have the rest of the s_i, the r_i follow immediately.

Let's put it this way, if we know how to solve a linear equation, we can use this method to solve a quadratic. If we know how to solve a quadratic, we can use this method to solve a cubic. Then we can use this method to solve a quartic, and so on.

The snag is, how do we calculate the coefficients of this polynomial. Suppose, given some power p, we have a set of s_i^p. If making a permutation of the r_i turns out to give us a permutation of the s_i^p, and that all possible permutations of the r_i lead to all possible permutations of the s_i^p then the s_i are functions of the coefficients of the original polynomial. This is because the the coefficients in the polynomial in s will be symmetric under permutations of the r_i. So, we can write down the coefficients of the polynomial in s in terms of the coefficients of the polynomial in x.

So, let's get back to our polynomial, and the discrete Fourier transform. No matter what the order of the polynomial is, the first coefficient is the sum of the roots, which gives us s_0. If we denote the N roots of unity as ζ_k, then the DFT looks like

$$s_k = \sum_{n=0}^{N-1} r_n \zeta_n^k. \tag{45}$$

For k=0, we have

$$s_0 = \sum_{n=0}^{N-1} r_n \zeta_n^0. \tag{46}$$

By definition $\zeta_n^0 = 1$. So, s_0 is just the sum of the roots, and will always be equal to the first coefficient of the polynomial.

5.1 The Quadratic

Let's see what we get with a quadratic equation.

$$x^2 + ax + b = (x - r_0)(x - r_1) = x^2 - (r_0 + r_1)x + r_0 r_1 = 0. \tag{47}$$

We just get another quadratic if we equate a and b with the expressions in the roots.

Our discrete Fourier transform and its inverse just uses the two square roots of one, ± 1. That is

$$\begin{aligned} s_0 &= (r_0 + r_1), \;\; r_0 = \frac{1}{2}(s_0 + s_1) \\ s_1 &= (r_0 - r_1), \;\; r_1 = \frac{1}{2}(s_0 - s_1) \end{aligned} \tag{48}$$

So for two numbers, the discrete transform and its inverse are very simple!

Now, this discrete Fourier transform gives us a unified approach to any polynomial as we shall see. In each case we obtain another equation called the *Lagrange resolvent*. It is obvious how we can find s_0 and s_1, but we can't use simple substitution for higher order cases. So, we won't use simple substitution for the quadratic.

The thing to notice here is what happens when we swap r_0 and r_1. The value of s_0 doesn't change of course, but s_1 changes sign. Now, the numbers a and b are invariant if we swap the roots about. We want to find the values for s_0 and s_1 in terms of a and b, so this change of sign in s_1 on swapping roots means that we are not there yet.

However, if we look at what happens to s_0^2 and s_1^2, these do not change if we swap r_0 and r_1. This symmetry property means that it is the square of s_1 that is the key to solving the equation. Now, eqn.59 tells us

$$\begin{aligned} s_1^2 &= (r_0 - r_1)^2 = (r_0^2 - 2r_0r_1 + r_1^2) \\ &= ((r_0 + r_1)^2 - 4r_0r_1) = (a^2 - 4b) \end{aligned} \tag{49}$$

It is trivial (in this case) but important to write down that s_1 is a solution of

$$(z^2 - s_1^2) = 0. \tag{50}$$

This is the Lagrange resolvent. Now we have s_0 and s_1, we can simply write down the roots using the inverse Fourier transform.

What has happened here? We have started off by writing down the quadratic as normal. Then we have written it down in terms of the unknown roots, and then wrote down the DFT of these two roots. Then we found that s_1 was not symmetric under the operation of swapping the roots, but that s_1^2 was. This meant that if we expanded s_1^2, in terms of the roots, we could find a simple expression for s_1^2 in terms of a and b. Though it hardly seemed worthwhile, we wrote down the Lagrange resolvent. Normally we would be looking at a higher order equation, and the resolvent equation would be a polynomial in z with coefficients found by finding a power of the s_i so that the resolvent polynomial invariant under *any* permutation of the roots. Then the power of the s_i have the same *symmetry group* as the r_i. This is what can enable us to find the s_i as functions of the coefficients. For the quadratic, we expect the solution to be a quadratic, so the power is two. For the cubic, we expect the solution to be in terms of cube roots, so the power is three. We shall see later that we don't actually need fourth powers for the quartic. With the quintic we are not lucky, but if it is to be solved in terms of radicals we expect an answer in terms of fifth roots, so the power will be five.

OK, that is an odd way of solving the the quadratic equation, but we have seen the simplest possible example of how the DFT of the roots can work. Why use this complex discrete Fourier transform rather than some other linear combination of roots? The answer to this question becomes clear on examining the cubic.

	ζ_0 ζ_1 ζ_2
ζ_0	ζ_0 ζ_1 ζ_2
ζ_1	ζ_1 ζ_2 ζ_0
ζ_2	ζ_2 ζ_0 ζ_1

Table 1: Multiplication table for the three cube roots of 1 ($\zeta_0 = 1$)

5.2 The Cubic

It turns out that finding formulae for coefficients in the Lagrange resolvent is very nasty, even though the actual formalae turn out to be simple in the end. We assume we have a depressed cubic to start with. That is

$$x^3 + ax + b = x^3 + (r_0r_1 + r_0r_2 + r_1r_2)x - r_0r_1r_2 = 0. \tag{51}$$

For cubic equations, our discrete Fourier transform needs the three cube roots of unity. That is $\zeta_0 = 1$, $\zeta_1 = -1/2 + \sqrt{3}/2\, i$, $\zeta_2 = -1/2 - \sqrt{3}/2\, i$. Now, when we substitute these in eqn.45, we shall come across things like $\zeta_1\zeta_2$ and ζ_2^2. We see the multiplication table in table 1. We see that ζ_0, ζ_1, ζ_2 form a group under the multiplication operator. Take any two members of the group of these three numbers and multiply them together and you get a member of the group. That is what makes our discrete Fourier transform more powerful than just any invertible linear combination of roots.

We add to our cursory introduction to groups by adding the following statements. We give a couple of examples of sets with an operation that are *not* closed under the operation, and so do not form groups. The set of numbers 1, 2, ... 10 does not form a group with the operator +, because 9+9=18 is not a member of the set. The set of negative integers does not form a group under the multiplication operator because (-2)×(-3)=6, which is not a negative integer and so is not a member of the set. Also, the set of integers under multiplication has an identity operator (1×), but not an inverse for every operation so it is *not* a group. (There is no inverse to 0×). Lastly, if a set of objects is closed under the operation, and there is an identity operation, and there is an inverse for every operation, it is still not a group if the operator is non-associative.

We want to solve

$$x^3 + ax^2 + bx + c = (x - r_0)(x - r_1)(x - r_2) = 0. \tag{52}$$

Our complex Fourier transform looks like

$$s_0 = \zeta_0^0 r_0 + \zeta_1^0 r_1 + \zeta_2^0 r_2$$

$$s_1 = \zeta_0^1 r_0 + \zeta_1^1 r_1 + \zeta_2^1 r_2$$

$$s_2 = \zeta_0^2 r_0 + \zeta_1^2 r_1 + \zeta_2^2 r_2 \tag{53}$$

but with our table, this is just

$$\begin{aligned} s_0 &= r_0 + r_1 + r_2 \\ s_1 &= r_0 + \zeta_1 r_1 + \zeta_2 r_2 \\ s_2 &= r_0 + \zeta_2 r_1 + \zeta_1 r_2 \end{aligned} \tag{54}$$

The inverse transform is just the complex conjugate of the transform, and $\zeta_1^* = \zeta_2$. So

$$\begin{aligned} 3r_0 &= s_0 + s_1 + s_2 \\ 3r_1 &= s_0 + \zeta_2 s_1 + \zeta_1 s_2 \\ 3r_2 &= s_0 + \zeta_2 s_1 + \zeta_1 s_2. \end{aligned} \tag{55}$$

So things look quite simple for the moment. As with the quadratic, if we swap any roots in the definition of s_0, nothing changes. Swapping r_1 and r_2 swaps the definition of s_1 and s_2, but look what happens if you swap r_0 and r_1. This isn't just a sign change. So s_1^2 and s_2^2 can't be simple functions of a, b, and c.

We have, in terms of the roots

$$s_1^3 = \left[r_1^3 + r_2^3 + r_3^3 + 6r_1r_2r_3 + 3\zeta_1(r_0r_2^2 + r_1r_0^2 + r_2r_1^2) + 3\zeta_2(r_0r_1^2 + r_1r_2^2 + r_2r_0^2)\right] \tag{56}$$

and

$$s_2^3 = \left[r_1^3 + r_2^3 + r_3^3 + 6r_1r_2r_3 + 3\zeta_2(r_0r_2^2 + r_1r_0^2 + r_2r_1^2) + 3\zeta_1(r_0r_1^2 + r_1r_2^2 + r_2r_0^2)\right]. \tag{57}$$

Now if we swap r_0 and r_1 we just have a swap of s_1 and s_2. So we expect

$$(z^3 - s_1^3)(z^3 - s_2^3) = z^6 - (s_1^3 + s_2)^3 z^3 + s_1^3 s_2^3 = 0 \tag{58}$$

to give us a polynomial with coefficients that depend on a and b. We don't mind the sixth power, as we view it as just a quadratic in z^3.

It was obvious what to do with the quadratic, but now things look very complicated indeed.

$$s_1^2 + s_2^3 = \left[2(r_1^3 + r_2^3 + r_3^3 + 6r_1r_2r_3) - 3(r_0r_2^2 + r_1r_0^2 + r_2r_1^2 - 3r_0r_1^2 + r_1r_2^2 + r_2r_0^2)\right]. \tag{59}$$

This is because $\zeta_1 + \zeta_2 = -1$. Now how can we proceed with this mess? First we note that if we just had $\zeta_2 = \zeta_1 = 1$ in eqns.56 and 57, we would have an expansion of $(r_1 + r_2 + r_3)^3$ for s_1^3 and s_2^3. So eqn.59 can be restated as

$$s_1^2 + s_2^3 = \left[2(r_0 + r_1 + r_2)^3 - 9(r_0r_2^2 + r_1r_0^2 + r_2r_1^2 + r_0r_1^2 + r_1r_2^2 + r_2r_0^2)\right]. \tag{60}$$

For our depressed cubic we have $r_0 + r_1 + r_2 = 0$. So we need to find out what

$$(r_0r_2^2 + r_1r_0^2 + r_2r_1^2 + r_0r_1^2 + r_1r_2^2 + r_2r_0^2). \tag{61}$$

can possibly be in terms of the coefficients a and b.

We already have $(r_0 + r_1 + r_2) = 0$. Let's examine the pair of terms

$$r_0 r_2^2 + r_2 r_0^2$$

$$= r_0(-r_1 - r_0)r_2 + r_2(-r_1 - r_2)r_0 =$$

$$-r_0 r_1 r_2 - r_2 r_0^2 - r_0 r_1 r_2 - r_0 r_2^2.$$

so

$$2(r_0 r_2^2 + r_2 r_0^2) = -2r_0 r_1 r_2 = +2b. \tag{62}$$

The same goes for other pairings, so all the terms in eqn.61 are just $3b$. So

$$s_1^3 + s_2^3 = +27 r_1 r_2 r_3 = -27b. \tag{63}$$

Now, when we multiply out the product $s_1^3 s_2^3$, we will get terms like r_0^6, how can we get such terms out of $r_1 r_2 r_3$ and $(r_0 r_1 + r_0 r_2 + r_1 r_2)$? Again, we look to $(r_0 + r_1 + r_2)$. This gives us

$$a = r_0 r_1 + r_0 r_2 + r_1 r_2 = -r_0(r_2 + r_0) - (r_1 + r_2)r_2 - r_1(r_0 + r_1)$$

$$= -[r_0^2 + r_1^2 + r_2^2 + r_0 r_1 + r_0 r_2 + r_1 r_2] \tag{64}$$

Suddenly, this looks interesting! We have

$$[r_0^2 + r_1^2 + r_2^2] = -2a. \tag{65}$$

When we expand $s_1^3 s_2^3$ it is obvious that we will get terms like $r_0^3 r_1^3$ and so we must have something in a^3 in the expansion. We note that

$$a^3 = [r_0(r_1 + r_2) + r_1 r_2]^3 = r_0^3(r_1 + r_2)^3 + 3r_0(r_1 + r_2)r_1^2 r_2^2 + 3r_0^2(r_1 + r_2)^2 r_1 r_2 + r_1^3 r_2^3.$$

$$= r_0^3 r_1^3 + r_0^3 r_2^3 + r_1^3 r_2^3$$

$$+3[(r_1 r_2^2 + r_1^2 r_2)r_0^3 + (r_0^2 r_2 + r_0 r_2^2)r_1^3 + (r_0^2 r_1 + r_1^2 r_0)r_2^3]$$

$$+6 r_0^2 r_1^2 r_2^2 \tag{66}$$

Hold on a moment! What's that term that looks like $6b^2 = 6r_0^2 r_1^2 r_2^2$? Since a and b are completely arbitrary coefficients, this cannot possibly be there! Of course, r_0, r_1, and r_2 are not independent. We must utilise $r_0 + r_1 + r_2 = 0$. From this we find

$$r_0^2 r_1^2 r_2^2 = -r_0(r_1 + r_2)r_1^2 r_2^2$$

from which

$$r_0^2 r_1^2 r_2^2 = -(r_0 r_2^2 r_1^3 + r_0 r_1^2 r_2^3). \tag{67}$$

If we write down all six possible permutations and add them together, we find

$$-6r_0^2 r_1^2 r_2^2 = +2[(r_1 r_2^2 + r_1^2 r_2)r_0^3 + (r_0^2 r_2 + r_0 r_2^2)r_1^3 + (r_0^2 r_1 + r_1^2 r_0)r_2^3], \tag{68}$$

so that

$$a^3 = r_0^3 r_1^3 + r_0^3 r_2^3 + r_1^3 r_2^3 + [(r_1 r_2^2 + r_1^2 r_2) r_0^3 + (r_0^2 r_2 + r_0 r_2^2) r_1^3 + (r_0^2 r_1 + r_1^2 r_0) r_2^3]. \quad (69)$$

Now, since $\zeta_1 + \zeta_2 = -1$, the product $s_1^3 s_2^3$ looks like

$$s_1^3 s_2^3 = (f + \zeta_1 g + \zeta_2 h)(f + \zeta_2 g + \zeta_1 h) = f^2 + g^2 + h^2 - (fg + gh + hf)$$

$$= (f + g + h)^2 - 3(fg + gh + hf) = (f + g + h)^2 - 3f(g + h) - 3gh, \quad (70)$$

Recall from eqn.57 that

$$f = (r_0^3 + r_1^3 + r_2^3 + 6 r_0 r_1 r_2)$$

and

$$g + h = -9 r_0 r_1 r_2 \quad (71)$$

We shall look at $(f + g + h)^2$ first

$$(f + g + h)^2 = (r_0^3 + r_1^3 + r_2^3 - 3 r_0 r_1 r_2)^2$$

$$= [r_0^6 + r_1^6 + r_2^6 + 2(r_0^3 r_1^3 + r_0^3 r_2^3 + r_1^3 r_2^3)]$$

$$-6(r_1 r_2 r_0^4 + r_0 r_2 r_1^4 + r_0 r_1 r_2^4) + 9 r_0^2 r_1^2 r_2^2 \quad (72)$$

Next we look at $f(g + h)$.

$$-3f(g + h) = 27 r_0 r_1 r_2 f = 27(r_0 r_1 r_2^4 + r_0 r_2 r_1^4 + r_1 r_2 r_0^4) + 162 r_0^2 r_1^2 r_2^2 \quad (73)$$

Finally we look at gh.

$$-3gh = -27(r_0 r_1 r_2^4 + r_0 r_2 r_1^4 + r_1 r_2 r_0^4)$$

$$-27(r_0^3 r_1^3 + r_0^3 r_2^3 + r_1^3 r_2^3) - 81 r_0^2 r_1^2 r_2^2. \quad (74)$$

So eqn.70 becomes

$$s_1^3 s_2^3 = r_0^6 + r_1^6 + r_2^6 - 25(r_0^3 r_1^3 + r_0^3 r_2^3 + r_1^3 r_2^3) - 6(r_1 r_2 r_0^4 + r_0 r_2 r_1^4 + r_0 r_1 r_2^4) + 90 r_0^2 r_1^2 r_2^2. \quad (75)$$

We notice that

$$r_0 r_1 r_2^4 = -(r_0 r_1^2 + r_1^2 r_0) r_2^3$$

so that

$$6 r_0^2 r_1^2 r_2^2 = 2(r_1 r_2 r_0^4 + r_0 r_2 r_1^4 + r_0 r_1 r_2^4). \quad (76)$$

Now we have

$$s_1^3 s_2^3 = r_0^6 + r_1^6 + r_2^6 - 25(r_0^3 r_1^3 + r_0^3 r_2^3 + r_1^3 r_2^3) + 24(r_1 r_2 r_0^4 + r_0 r_2 r_1^4 + r_0 r_1 r_2^4). \quad (77)$$

We can use $r_0 + r_1 + r_2 = 0$ to write

$$r_0^6 + r_1^6 + r_2^6 = -2(r_0^3 r_1^3 + r_0^3 r_1^3 + r_1^3 r_2^3) - 3[(r_0^2 r_1 + r_0 r_1^2) r_2^3 + (r_0^2 r_2 + r_0 r_2^2) r_1^3 + (r_1^2 r_1 + r_1 r_1^2) r_0^3]. \quad (78)$$

Also

$$r_1r_2r_0^4 + r_0r_2r_1^4 + r_0r_1r_2^4 = -[(r_0^2r_1 + r_0r_1^2)r_2^3 + (r_0^2r_2 + r_0r_2^2)r_1^3 + (r_1^2r_1 + r_1r_1^2)r_0^3]. \quad (79)$$

So we now have

$$s_1^3s_2^3 = -27(r_0^3r_1^3 + r_0^3r_2^3 + r_1^3r_2^3) - 27[(r_0^2r_1 + r_0r_1^2)r_2^3 + (r_0^2r_2 + r_0r_2^2)r_1^3 + (r_1^2r_1 + r_1r_1^2)r_0^3]. \quad (80)$$

So, on looking at eqn.66, all that complicated algebra just boils down to

$$s_1^3s_2^3 = -27a^3. \quad (81)$$

Our Lagrange resolvent is just

$$s^6 + 27bs^3 - 27a^3 = 0. \quad (82)$$

The resolvent that gives us s_1 and s_2 is a quadratic in s^3. Now we have yet another problem, on solving the resolvent we have s_1^3 and s_2^3, but we now have three possible values for s_1 and three values for s_2. We shall go no further here, but obviously trial and error as to which roots work is always possible.

5.3 The Quartic

We write down the depressed quartic equation in terms of the unknown roots and the given coefficients.

$$x^4 + ax^2 + bx + c = (x - r_3)(x - r_2)(x - r_1)(x - r_0) = 0. \quad (83)$$

We already have the product of the last three terms from the cubic. So

$$x^4 + ax^2 + bx + c = x^4 - (r_0 + r_1 + r_2 + r_3)x^3$$

$$+(r_0r_1 + r_0r_2 + r_1r_2 + r_0r_3 + r_1r_3 + r_2r_3)x^2$$

$$-(r_0r_1r_2 + r_3r_0r_1 + r_3r_0r_2 + r_3r_1r_2)x + r_0r_1r_2r_3 = 0. \quad (84)$$

Because we already have a depressed quartic, we know that $r_0 + r_1 + r_2 + r_3 = 0$.

Now, the four fourth roots of one are just $\pm 1, \pm i$. The discrete Fourier transform

$$s_0 = \zeta_0^0 r_0 + \zeta_1^0 r_1 + \zeta_2^0 r_2 + \zeta_3^0 r_3$$

$$s_1 = \zeta_0^1 r_0 + \zeta_1^1 r_1 + \zeta_2^1 r_2 + \zeta_3^1 r_3$$

$$s_2 = \zeta_0^2 r_0 + \zeta_1^2 r_1 + \zeta_2^2 r_2 + \zeta_3^2 r_3$$

$$s_2 = \zeta_0^3 r_0 + \zeta_1^3 r_1 + \zeta_2^3 r_2 + \zeta_3^3 r_3 \quad (85)$$

is just

$$s_0 = r_0 + r_1 + r_2 + r_3$$

$$s_1 = r_0 + r_1 i - r_2 - r_3 i$$
$$s_2 = r_0 - r_1 + r_2 - r_3$$
$$s_3 = r_0 - r_1 i - r_2 + r_3 i. \tag{86}$$

There is a peculiarity here. If we write this down in matrix form, we can immediately write down the inverse. When we multiply out the matrix and its inverse it makes no difference if we replace i with one. In this case it is advantageous to do exactly that, and write

$$s_0 = r_0 + r_1 + r_2 + r_3,$$
$$s_1 = r_0 + r_1 - r_2 - r_3,$$
$$s_2 = r_0 - r_1 + r_2 - r_3,$$
$$s_3 = r_0 - r_1 - r_2 + r_3. \tag{87}$$

If we had defined the DFT as having a factor of $1/\sqrt{N}$, then the the inverse transform would also have a factor of $1/\sqrt{N}$, we would have had a more symmetric version of the DFT. This would be a *unitary transform* with $UU^* = I$ (the identity matrix). We now swap over to this symmetric form, and now use eqn.88 instead of eqn.87. If we write this in matrix form, the matrix would be its own inverse. This kind of transform is called an *involution*.

$$s_0 = \frac{1}{2}(r_0 + r_1 + r_2 + r_3),$$
$$s_1 = \frac{1}{2}(r_0 + r_1 - r_2 - r_3),$$
$$s_2 = \frac{1}{2}(r_0 - r_1 + r_2 - r_3),$$
$$s_3 = \frac{1}{2}(r_0 - r_1 - r_2 + r_3). \tag{88}$$

Taking squares we have

$$s_1^2 = \frac{1}{4}[r_0^2 + r_1^2 + r_2^2 + r_3^2 + 2(r_0 r_1 - r_0 r_2 - r_0 r_3 - r_1 r_2 - r_1 r_3 + r_2 r_3)],$$
$$s_2^2 = \frac{1}{4}[r_0^2 + r_1^2 + r_2^2 + r_3^2 + 2(-r_0 r_1 + r_0 r_2 - r_0 r_3 - r_1 r_2 + r_1 r_3 - r_2 r_3)],$$
$$s_3^2 = \frac{1}{4}[r_0^2 + r_1^2 + r_2^2 + r_3^2 + 2(-r_0 r_1 - r_0 r_2 + r_0 r_3 + r_1 r_2 - r_1 r_3 - r_2 r_3)]. \tag{89}$$

If we swap r_0 and r_1

$$s_1^2 \to \frac{1}{4}[r_0^2 + r_1^2 + r_2^2 + r_3^2 + 2(r_0 r_1 - r_0 r_2 - r_0 r_3 - r_1 r_2 - r_1 r_3 + r_2 r_3)],$$
$$s_2^2 \to \frac{1}{4}[r_0^2 + r_1^2 + r_2^2 + r_3^2 + 2(-r_0 r_1 - r_0 r_2 + r_0 r_3 + r_1 r_2 - r_1 r_3 - r_2 r_3)],$$
$$s_3^2 =\to \frac{1}{4}[r_0^2 + r_1^2 + r_2^2 + r_3^2 + 2(-r_0 r_1 + r_0 r_2 - r_0 r_3 - r_1 r_2 + r_1 r_3 - r_2 r_3)]. \tag{90}$$

We have, on swapping r_0 and r_1, $s_2^2 \rightarrow s_3^2$, and $s_3^2 \rightarrow s_2^2$, with s_1^2 unchanged. Similarly swapping r_0 and r_2 swaps s_1^2 and s_2^2; swapping r_0 and r_3 swaps s_1^2 and s_3^2; swapping r_1 and r_2 swaps s_1^2 and s_3^2; swapping r_1 and r_3 swaps s_1^2 and s_2^2; and swapping r_2 and r_3 swaps s_2^2 and s_3^2.

The coefficients of

$$(s^2 - s_1^2)(s^2 - s_2^2)(s^2 - s_3^2)$$

$$= s^6 - (s_1^2 + s_2^2 + s_3^2)s^4 + (s_1^2 s_2^2 + s_1^2 s_3^2 + s_2^2 s_3^2)s^2 - s_1^2 s_2^2 s_3^2 = 0, \tag{91}$$

are symmetric with respect to any swap of the s_i, and symmetric with any swap of the r_i. So, the coefficients of eqn.91 will be functions of a, b, and c.

If we hadn't done our "trick" of replacing i with 1 in the transform and its inverse, we would have had to have expanded up to s_i^4 to get the right symmetry. This trick makes the ensuing algebra much less complicated than it would have been otherwise.

Now looking at eqn.91, the coefficient of s^4 is

$$s_1^2 + s_2^2 + s_3^2 = \frac{1}{4}[3(r_0^2 + r_1^2 + r_2^2 + r_3^2)$$

$$-2(r_0 r_1 + r_0 r_2 + r_0 r_3 + r_1 r_2 + r_1 r_3 + r_2 r_3)]. \tag{92}$$

If we substitute $r_0 + r_1 + r_2 + r_3 = 0$ into the sum of the squares of the roots, we find that

$$r_0^2 + r_1^2 + r_2^2 + r_3^2 = -2(r_0 r_1 + r_0 r_2 + r_0 r_3 + r_1 r_2 + r_1 r_3 + r_2 r_3). \tag{93}$$

So, from eqn.84, eqn.92, and eqn.93 we have

$$s_1^2 + s_2^2 + s_3^2 = -2(r_0 r_1 + r_0 r_2 + r_0 r_3 + r_1 r_2 + r_1 r_3 + r_2 r_3) = -2a. \tag{94}$$

Let's have a look at the coefficient of s^2 in eqn.91. First we can use eqn.93 to simplify eqn.89 to

$$s_1^2 = -(r_0 r_2 + r_0 r_3 + r_1 r_2 + r_1 r_3),$$

$$s_2^2 = -(r_0 r_1 + r_0 r_3 + r_1 r_2 + r_2 r_3),$$

$$s_3^2 = -(r_0 r_1 + r_0 r_2 + r_1 r_3 + r_2 r_3). \tag{95}$$

Then

$$s_1^2 s_2^2 + s_1^2 s_3^2 + s_2^2 s_3^2 = r_0^2 r_1^2 + r_0^2 r_2^2 + r_0^2 r_3^2 + r_1^2 r_2^2 + r_1^2 r_3^2 + r_2^2 r_3^2$$

$$+3r_0^2(r_1 r_2 + r_1 r_3 + r_2 r_3) + 3r_1^2(r_0 r_2 + r_0 r_3 + r_2 r_3)$$

$$+3r_2^2(r_0 r_1 + r_0 r_3 + r_1 r_3) + 3r_3^2(r_0 r_1 + r_0 r_2 + r_1 r_2) + 6r_0 r_1 r_2 r_3. \tag{96}$$

We note from eqn.84 that

$$a^2 = r_0^2 r_1^2 + r_0^2 r_2^2 + r_0^2 r_3^2 + r_1^2 r_2^2 + r_1^2 r_3^2 + r_2^2 r_3^2$$

$$+2r_0^2(r_1 r_2 + r_1 r_3 + r_2 r_3) + 2r_1^2(r_0 r_2 + r_0 r_3 + r_2 r_3)$$

$$+2r_2^2(r_0r_1+r_0r_3+r_1r_3)+2r_3^2(r_0r_1+r_0r_2+r_1r_2)+6r_0r_1r_2r_3. \tag{97}$$

We also note that, because the roots sum to zero,

$$r_0r_1r_2r_3=-(r_1^2r_2r_3+r_2^2r_1r_3+r_3^2r_1r_2). \tag{98}$$

This was just substituting for r_0. If we do similar substitutions for r_1, r_2, and r_3 we see that

$$\begin{aligned}4r_0r_1r_2r_3=&-r_0^2(r_1r_2+r_1r_3+r_2r_3)-r_1^2(r_0r_2+r_0r_3+r_2r_3)\\&-r_2^2(r_0r_1+r_0r_3+r_1r_3)-r_3^2(r_0r_1+r_0r_2+r_1r_2).\end{aligned} \tag{99}$$

So, eqn.96 now looks like

$$s_1^2s_2^2+s_1^2s_3^2+s_2^2s_3^2=a^2-4r_0r_1r_2r_3=a^2-4c. \tag{100}$$

Last of all we must examine $s_1^2s_2^2s_3^2$. This will generate homogeneous terms of degree six. We can get terms like that from a^3 or b^2.

$$\begin{aligned}b^2=&\,r_0^2r_1^2r_2^2+r_0^2r_1^2r_3^2+r_0^2r_2^2r_3^2+r_1^2r_2^2r_3^2\\&+2(r_0^2r_1^2r_2r_3+r_0^2r_2^2r_1r_3+r_0^2r_3^2r_1r_2+r_1^2r_2^2r_0r_3+r_1^2r_3^2r_0r_2+r_2^2r_3^2r_0r_1).\end{aligned} \tag{101}$$

If we just expand $s_1^2s_2^2s_3^2$. This gives us

$$\begin{aligned}-s_1^2s_2^2s_3^2=&\,r_0^3[r_1^2(r_2+r_3)+r_2^2(r_1+r_3)+r_3^2(r_1+r_2)+2r_1r_2r_3]\\&+r_1^3[r_0^2(r_2+r_3)+r_2^2(r_0+r_3)+r_3^2(r_0+r_2)+2r_0r_2r_3]\\&+r_2^3[r_0^2(r_1+r_3)+r_1^2(r_0+r_3)+r_3^2(r_0+r_1)+2r_0r_1r_3]\\&+r_3^3[r_0^2(r_1+r_2)+r_1^2(r_0+r_2)+r_2^2(r_0+r_1)+2r_0r_1r_2]\\&+2r_0^2(r_1^2r_2r_3+r_2^2r_1r_3+r_3^2r_1r_2)+2r_1^2(r_0^2r_2r_3+r_3^2r_1r_2+r_2^2r_0r_3)\\&+2r_2^2(r_0^2r_1r_3+r_3^2r_0r_1+r_1^2r_0r_3)+2r_3^2(r_1^2r_0r_3+r_2^2r_0r_1+r_0^2r_1r_2)\\&+2(r_0^2r_1^2r_2^2+r_0^2r_1^2r_3^2+r_0^2r_2^2r_3^2+r_1^2r_2^2r_3^2).\end{aligned} \tag{102}$$

All this doesn't look very friendly, however, lets put

$$\begin{aligned}X=&\,r_0^3[r_1^2(r_2+r_3)+r_2^2(r_1+r_3)+r_3^2(r_1+r_2)+2r_1r_2r_3]\\&+r_1^3[r_0^2(r_2+r_3)+r_2^2(r_0+r_3)+r_3^2(r_0+r_2)+2r_0r_2r_3]\\&+r_2^3[r_0^2(r_1+r_3)+r_1^2(r_0+r_3)+r_3^2(r_0+r_1)+2r_0r_1r_3]\\&+r_3^3[r_0^2(r_1+r_2)+r_1^2(r_0+r_2)+r_2^2(r_0+r_1)+2r_0r_1r_2].\end{aligned} \tag{103}$$

Now, if we put $r_0^3=-r_0^2(r_1+r_2+r_3)$ and so on, in all the r_i^3 terms, we get

$$X=-r_0^3(r_1^2(r_2+r_3)+r_2^2(r_1+r_3)+r_3^2(r_1+r_2))-r_1^3(r_0^2(r_2+r_3)+r_2^2(r_0+r_3)+r_3^2(r_0+r_2))$$

$$-r_2^3(r_0^2(r_1+r_3)+r_1^2(r_0+r_3)+r_3^2(r_0+r_1))-r_3^3(r_0^2(r_1+r_2)+r_1^2(r_0+r_2)+r_2^2(r_0+r_1))$$
$$-6(r_0^2r_1^2r_2^2+r_0^2r_1^2r_3^2+r_0^2r_2^2r_3^2+r_1^2r_2^2r_3^2)$$
$$-4r_0^2(r_1^2r_2r_3+r_2^2r_1r_3+r_3^2r_1r_2)-4r_1^2(r_0^2r_2r_3+r_3^2r_1r_2+r_2^2r_0r_3)$$
$$-4r_2^2(r_0^2r_1r_3+r_3^2r_0r_1+r_1^2r_0r_3)-4r_3^2(r_1^2r_0r_3+r_2^2r_0r_1+r_0^2r_1r_2). \quad (104)$$

If we add eqn.103 to 104, we get

$$X=(r_0^3r_1r_2r_3+r_1^3r_0r_2r_3+r_2^3r_0r_1r_3+r_3^2r_0r_1r_2)$$
$$-3(r_0^2r_1^2r_2^2+r_0^2r_1^2r_3^2+r_0^2r_2^2r_3^2+r_1^2r_2^2r_3^2)$$
$$-2r_0^2(r_1^2r_2r_3+r_2^2r_1r_3+r_3^2r_1r_2)-2r_1^2(r_0^2r_2r_3+r_3^2r_1r_2+r_2^2r_0r_3)$$
$$-2r_2^2(r_0^2r_1r_3+r_3^2r_0r_1+r_1^2r_0r_3)-2r_3^2(r_1^2r_0r_3+r_2^2r_0r_1+r_0^2r_1r_2). \quad (105)$$

After this eqn.102 simplifies to

$$-s_1^2s_2^2s_3^2=(r_0^3r_1r_2r_3+r_1^3r_0r_2r_3+r_2^3r_0r_1r_3+r_3^2r_0r_1r_2)$$
$$-(r_0^2r_1^2r_2^2+r_0^2r_1^2r_3^2+r_0^2r_2^2r_3^2+r_1^2r_2^2r_3^2). \quad (106)$$

Now, one last application of $r_1+r_2+r_3+r_4=0$ gives us

$$-s_1^2s_2^2s_3^2=-2(r_0^2r_1^2r_2r_3+r_0^2r_2^2r_1r_3+r_0^2r_3^2r_1r_2+r_1^2r_2^2r_0r_3+r_1^2r_3^2r_0r_2+r_2^2r_3^2r_0r_1)$$
$$-(r_0^2r_1^2r_2^2+r_0^2r_1^2r_3^2+r_0^2r_2^2r_3^2+r_1^2r_2^2r_3^2). \quad (107)$$

On recalling eqn.101, our resolvent equation is

$$s^6+2as^4+(a^2-4c)s^2-b^2=0. \quad (108)$$

6 The Quintic Equation Train-Wreck

For the quadratic, the two roots are a linear combination of the s_i, which are the square roots of the solution of the resolvent $s^2-s_1^2=0$. For the cubic, the roots are a linear combination of the s_i, which are the cube roots of the solution of resolvent equation $s^6+27bs^3-27c=0$. The solution of the cubic in §3.1 assumes a solution as a linear combination of cube roots in just this way. All we do here can be done without the DFT, but the DFT makes a neat job of things. In the quartic, our "trick" gave us a solution in terms of the s_i which are the square roots of the cubic equation $s^6+2as^4+(a^2-4c)s^2-b^2=0$.

We shall now stand things on their head as it were and make the following observation. Consider the cubic and the quadratic. We could have *generated* the other s_i^p from s_1^p by swapping the roots. In the case of the cubic, we would either get s_1^3 or s_2^3 whatever the permutation, and so the resolvent is a quadratic. In the quartic, we would always get s_1^2, s_2^2 or s_3^2 no matter what permutation of the roots, and the resolvent must be a cubic.

	$1\ \zeta_1\ \zeta_2\ \zeta_3\ \zeta_4$
1	$1\ \zeta_1\ \zeta_2\ \zeta_3\ \zeta_4$
ζ_1	$\zeta_1\ \zeta_2\ \zeta_3\ \zeta_4\ 1$
ζ_2	$\zeta_2\ \zeta_3\ \zeta_4\ 1\ \zeta_1$
ζ_3	$\zeta_3\ \zeta_4\ 1\ \zeta_1\ \zeta_2$
ζ_4	$\zeta_4\ 1\ \zeta_1\ \zeta_2\ \zeta_3$

Table 2: Multiplication table for the five fifth roots of 1 ($\zeta_0 = 1$)

6.1 The DFT for the Quintic

We mentioned in the introduction, that algebraic methods in general fail for the general quintic and beyond. We shall see why when we take a look at what happens if we try the DFT method used here so far.

$$\begin{aligned}
s_0 &= \zeta_0^0 r_0 + \zeta_1^0 r_1 + \zeta_2^0 r_2 + \zeta_3^0 r_3 + \zeta_4^0 r_4 \\
s_1 &= \zeta_0^1 r_0 + \zeta_1^1 r_1 + \zeta_2^1 r_2 + \zeta_3^1 r_3 + \zeta_4^1 r_4 \\
s_2 &= \zeta_0^2 r_0 + \zeta_1^2 r_1 + \zeta_2^2 r_2 + \zeta_3^2 r_3 + \zeta_4^2 r_4 \\
s_3 &= \zeta_0^3 r_0 + \zeta_1^3 r_1 + \zeta_2^3 r_2 + \zeta_3^3 r_3 + \zeta_4^3 r_4 \\
s_4 &= \zeta_0^4 r_0 + \zeta_1^4 r_1 + \zeta_2^4 r_2 + \zeta_3^4 r_3 + \zeta_4^4 r_4.
\end{aligned} \tag{109}$$

As always, $\zeta_0 = 1$. The roots of one are at the vertices of a pentagon in the complex plane. We recall the Golden Ratios $\phi = (\sqrt{5}-1)/2$ and $\Phi = (\sqrt{5}+1)/2$, with $\Phi - \phi = 1$. Then we put $\zeta_1 = \cos 72^\circ - \sin 72^\circ i$, $\zeta_2 = -\cos 36^\circ - \sin 36^\circ i$, $\zeta_3 = \zeta_2^*$, and $\zeta_4 = \zeta_1^*$. We also know that $\cos 72^\circ = \phi/2$, $\cos 36^\circ = \Phi/2$, $\sin 72^\circ = \sqrt{(2+\Phi)}/2$, $\sin 72 = \sqrt{(2-\phi)}/2$. Our multiplication table is shown in table 2. So we can write our DFT as

$$\begin{aligned}
s_0 &= r_0 + r_1 + r_2 + r_3 + r_4 \\
s_1 &= r_0 + \zeta_1 r_1 + \zeta_2 r_2 + \zeta_3 r_3 + \zeta_4 r_4 \\
s_2 &= r_0 + \zeta_2 r_1 + \zeta_4 r_2 + \zeta_1 r_3 + \zeta_3 r_4 \\
s_3 &= r_0 + \zeta_3 r_1 + \zeta_1 r_2 + \zeta_4 r_3 + \zeta_2 r_4 \\
s_4 &= r_0 + \zeta_4 r_1 + \zeta_3 r_2 + \zeta_2 r_3 + \zeta_1 r_4.
\end{aligned} \tag{110}$$

We shall look at $s = a + \zeta_1 b + \zeta_2 c + \zeta_3 d + \zeta_4 e$.

$$s^5 = [a^5+b^5+c^5+d^5+e^5+20(ab^3c+ac^3e+ad^3e+abd^3+a^3be+bce^3+bc^3d+a^3cd+cd^3e+b^3de)$$

$$+30(a^2bc^2+a^2b^2d+a^2d^2e+a^2ce^2+b^2c^2e+b^2cd^2+ab^2e^2+ac^2d^2+c^2de^2+bd^2e^2)+120abcde]$$

$$+\zeta_1[5(a^4b+b^4c+c^4d+d^4e+ae^4)+20(a^3ce+ab^3d+bc^3e+acd^3+bde^3)$$

$$+10(a^3d^2+b^3e^2+a^2c^3+b^2d^3+c^2e^3)+30(ab^2c^2+bc^2d^2+cd^2e^2+a^2de^2+a^2b^2e)$$
$$+60(a^2bcd+b^2cde+ac^2de+abd^2e+abce^2)]$$
$$+\zeta_2[5(a^4c+b^4d+c^4e+ad^4+be^4)+20(a^3de+ab^3e+abc^3+bcd^3+cde^3)$$
$$+10(a^3b^2+b^3c^2+c^3d^2+d^3e^2+a^2e^3)+30(ac^2e^2+a^2bd^2+a^2c^2d+b^2d^2e+b^2ce^2)$$
$$+60(a^2bce+ab^2cd+bc^2de+acd^2e+abde^2)]$$
$$+\zeta_3[5(a^4d+b^4e+ac^4+bd^4+ce^4)+20(a^3bc+b^3cd+c^3de+ad^3e+abe^3)$$
$$+10(a^3e^2+a^2b^3+b^2c^3+c^2d^3+d^2e^3)+30(ab^2d^2+bc^2e^2+b^2de^2+a^2cd^2+a^2c^2e)$$
$$+60(a^2bde+ab^2ce+abc^2d+bcd^2e+acde^2)]$$
$$+\zeta_4[5(a^4e+ab^4+bc^4+cd^4+de^4)+20(a^3bd+b^3ce+ac^3d+bd^3e+ace^3)$$
$$+10(a^3c^2+b^3d^2+c^3e^2+a^2d^3+b^2e^3)+30(ad^2e^2+ba^2e^2+a^2b^2c+b^2cd^2+c^2d^2e)$$
$$+60(a^2cde+ab^2de+abc^2e+abcd^2e+bcde^2)]. \tag{111}$$

Now, in eqn.110 we have $(a,b,c,d,e) = (r_0,r_1,r_2,r_3,r_4)$ for s_1^5, similarly, we have $(a,b,c,d,e) = (r_0,r_3,r_1,r_4,r_3)$ for s_2^5 and so on. Suppose we start with just s_1^5, and *generate* other s_i^5 by permuting the roots. The lack of nice symmetries in eqn.111 means that we generate 24 s_i^5s. The resolvent equation is of far higher degree than the original quintic!

6.2 More Groups

Let's go back to group theory, and examine the *Symmetric group* S_3. If we have 3 elements $1,2,3$ then S_3 is the group of permutations of the elements. One permutation may be written

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \tag{112}$$

Which just means what is in column 1 moves to column 3, The content of column 2 stays as it is, and what is in column 3 moves to column 1. Most often, this kind of thing is written on one line in *cycle notation*. To do this we write down a "(", next we write down the first column number in columns (1,2,3) that is changed, so we have "(1". Now the one in column 1 goes to column 3 so we write "(1,3". Then 3 goes to 1, but this takes us back to 1 and we would go on repeating if we continued. When we reach a repetition like this we close the parentheses so we now have (1,3). We then repeat this procedure on the what is left. Only 2 is left, but that isn't mapped to anything, so we write this as (1,3)(2) or more usually just (1,3). If the operation maps 1 to 1, 2 to 2, and 3 to 3, then there isn't a first changed number. This is operation is just denoted as () which is the identity. In this notation we have (), (2,3), (1,2), (1,2,3), (1,3,2) and (1,3) for the six possible permutations on 123.

	()	(1,2)	(2,3)	(1,3)	(1,2,3)	(1,3,2)
()	()	(1,2)	(2,3)	(1,3)	(1,2,3)	1,3,2)
(1,2)	(1,2)	()	(1,2,3)	(1,3,2)	(2,3)	(1,3)
(2,3)	(2,3)	(1,3,2)	()	(1,2,3)	(1,3)	(1,2)
(1,3)	(1,3)	(1,2,3)	(1,3,2)	()	(1,2)	(2,3)
(1,2,3)	(1,2,3)	(1,3)	(1,2)	(2,3)	(1,3,2)	()
(1,3,2)	(1,3,2)	(2,3)	(1,3)	(1,2)	()	(1,2,3)

Table 3: Table for the Symmetric Group $S3$

Note there is a shift here, instead of having a set of numbers or symbols, we now have a *set of operators*. The set along with the operation of *combining operations* is thus a type of group we haven't seen before. Table 3 is a group table for the permutation operators on three symbols. The group S_3 is of order 6. Any combination of two operators is equivalent to another single operation that is a member of the group of operations. That is, the group is a *bijective* map onto itself. We note that $(1,2)(2,3) \neq (2,3)(1,2)$, so the group is said to be *non abelian*. (The term abelian is named after Abel). It is also *isomorphic* to the symmetry group of the equilateral triangle. That is, the two different groups have exactly the same structure. Here (1,2,3) and (1,3,2) are equivalent to rotations, and the other operators are equivalent to flips about the points (or reflections). We note also that S_3 has the two rotations (together with the identity) as a *normal subgroup* of order 3. A subgroup in general can include the group itself, a normal subgroup does not. There is always the *trivial subgroup* — the identity element. (Often, the identity is denoted e or E.) The identity, along with (1,2,3) (1,3,2) form the *cyclic group* C_3.

A *transposition* is a permutation consisting of only a pair swap such as (1,3). Absolutely *any* permutation can be written as a sequence of transpositions. A permutation is said to be *odd* if it can be written as an odd number of transpositions, and *even* if it can be written as an even number of transpositions. The permutation can be assigned the value $+1$ for even permutations and -1 for odd permutations. It follows that the set of even permutations of the symmetric group S_N is a normal subgroup of S_N. This is denoted A_N and is called the *alternating group*. (Obviously the odd permutations do not form a subgroup since an odd permutation of an odd permutation is even.) We can see that in S_3 that the A_3 are the rotations. That is $A_3 = C_3$.

Looking at S_4, we have following elements. The identity is even (), then (3,4), (2,3), (2,4), (1,2), (1,3), (1,4) are odd. Then we have (2,4,3), (2,3,4), (1,3,2), (1,4,2), (1,2,3), (1,4,3), (1,2,4), and (1,3,4), which are all even. Then we have a set of double transpositions (even) consisting of (1,2)(3,4), (1,3)(2,4), and (1,4)(2,3). Finally there are the odd permutations (1,4,3,2), (3,4,2,1), (1,2,4,3), (1,4,2,3), (1,2,3,4), and (1,3,2,4). So, S_4 has A_4 as a normal subgroup. If we examine the three transposition pairs we see that, for instance,

[(1,2)(3,4)][(1,3)(2,4)]=(1,4)(2,3), and so on. That is these three operators along with the identity form a normal subgroup of A_4. This group is known as the *Klein Viergruppe* and is denoted V. The Viergruppe is abelian. The reader may check that, if we take the set of numbers 1,2,3,4 and construct a table with the operators of S_3 exactly as described above for the top row, and the operators for V in the left column, then we get all the permutations of S_4. That is $S_4 = V \times S_3$. Note that V has a subgroup consisting of the identity and (1,2)(3,3).

The symmetric group S_4 is isomorphic to the symmetry group of the cube. This has three rotations of $\pm\pi/2$ or π radians about opposite centres of pairs of faces. A rotation of π around 6 pairs of opposite edges, rotations of $\pm 2\pi/3$ about 4 pairs of opposite vertices. That is 9+6+8 operations, plus the identity, making 24. What exactly are these four objects that are permuted when we rotate a cube? We have 8 vertices, 12 edges, and 6 faces. If we examine the rotations in detail, we find that the four long diagonals are permuted by a rotation.

The dodecahedron has 4 rotations with multiples of $\pm 2\pi/5$ about centres of 6 pairs of opposite faces, one rotation of π about 15 pairs of opposite edges, two rotations (of $\pm 2\pi/3$) about 10 pairs of opposite vertices, plus the identity, making 60 elements. The alternating group A_5 is isomorphic to the symmetry group of the dodecahedron (or icosahedron) and is a normal subgroup of S_5. Again, we ask the question, what are the five objects being permuted here? Again, a close examination shows that there are five cubes "hiding" in the dodecahedron (see Fig.1), and these are permuted by rotations. However the rotations only give rise to even permutations so we get A_5 rather than the full dodecaheral (or icosahedral) group I_h. The full icosahedral group of order 120 is $I_h = C_2 \times A_5$. (The full group includes combined reflection and rotation operations.) Confusingly, though S_5 and I_h are both of degree 120, and both have A_5 as a proper subgroup, *they are not isomorphic*.

There is a major difference between S_5 and the lower symmetric groups. It cannot be broken down into a sequence of smaller and smaller subgroups. This is what lies at the core of the insolvability of the quintic in terms of radicals. For the quadratic, $S_2 = C_2$ operating on the roots mapped to the identity operating on s_1. The identity is of course a normal subgroup of S_2. For the cubic S_3 acting on the roots became $C_2 = S_3/A_3$ or $C_2 = S_3/C_3$ acting on (s_1, s_2). For the quartic we had S_4 acting on the roots, and this became $S_3 = S_4/V$ acting on (s_1, s_2, s_3). In each case, there was a normal subgroup of the initial symmetric group of the right order to operate on the $N-1$ s_i. S_5 has only E, and A_5 as normal subgroups, that's why it's "game over". There is no normal subgroup of order 4 to operate on s_1, s_2, s_3, s_4. If a subset of S_5 is not a subgroup of order 4, it will generate terms not in the set (s_1, s_2, s_3, s_4), hence we get all the way up to s_{24}.

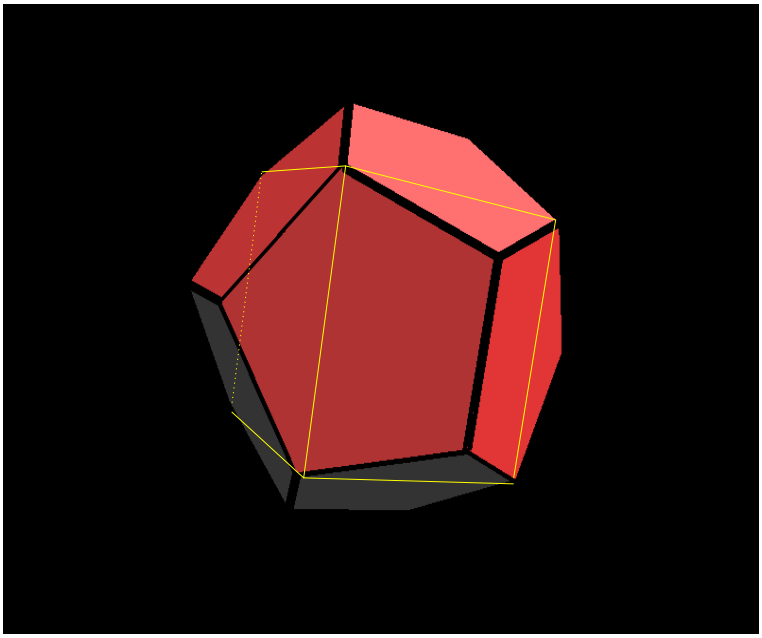

Figure 1: Two facets of one of the five inscribed cubes possible for a dodecahedron.

7 Solving Polynomials for Practical Purposes

First of all, the general quintic *is* solvable, but not in terms of radicals. There are all sorts of advanced methods of which the author knows nothing (apart from their existence) which can cope with quintics and higher order polynomials.

There are many numerical techniques for solving polynomials, but we shall only mention one. Most methods involve a "first guess" at a root, followed by an iterative algorithm that takes the guess closer and closer to the actual root. However one method can give us all the roots, real and complex, of any order of polynomial, all in go. Given the polynomial

$$P = x^n + a_{n-1}x^{n-1} \ \ldots \ a_2x^2 + a_1x + a_0 = 0, \tag{113}$$

we can define the $N \times N$ *companion matrix* C as

$$C(P) = \begin{pmatrix} 0 & 0 & 0 & 0 & \ldots & 0 & a_0 \\ 1 & 0 & 0 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & 0 & 0 & \ldots & 0 & a_2 \\ 0 & 0 & 1 & 0 & \ldots & 0 & a_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 1 & a_{n-1} \end{pmatrix}. \tag{114}$$

The *eigenvalues* of the companion matrix are the roots of $P(x)$. So, if we have a linear algebra package such as $LAPACK$, we can use an appropriate routine to calculate all the roots, real and complex, in one call. (Naturally a sparse matrix routine is preferred for high order polynomials.)

8 A Potted History

The first algorithms for working out square and cube roots date back to Argabhata in India (around 500BC). The first cubic equations ever solved were special cases where it was possible to complete the cube. This goes back to Bhaskara, again in India (1150 AD). At around this time much work on the cubic equation was done in Persia. Here for instance, the polymath Omar Khayyám (still famous in the west for his poem the Rubaiyat) found a geometrical construction to provide one root of a cubic. Omar Kayyám (1028-1143) is the first person known to have considered the quintic equation.

Luca Pacioli (1445-1509) declared the general solution of the cubic equation to be impossible. However Scipione del Ferro (1465-1526) found a general solution, which he kept secret (for reasons mentioned earlier). He did confide the secret to Antoni Maria Fior, and Annibale della Nave, when we retired. This was so Fior could succeed him as professor. Tartaglia (1500-1557) solved the general cubic independently. Fior could only solve the depressed cubic, and Tartaglia successfully challenged Fior in 1535. (Tartaglia means "the stammerer": he had a speech impediment because of a sabre slash received as a boy during Gaston du Foix's vicious sack of Brescia during which some 45 000 residents of the town were killed. Tartaglia's real name was Nicollò Fontana.)

Gerolamo Cardano (1501-1576) got Tartaglia to tell him the secret of the cubic, and was sworn to secrecy. But he discovered from Nave, that del Ferro had the general solution before Tartaglia, and so Cardano published it in the *Ars Magna*. Cardano's student Lodovico Ferrari (1522-1565) solved the quartic equation at this time.

One can imagine that many mathematicians would want to be the first to find a general method of solving the quintic. Work by François Viète (1540-1603) showed how sums of powers of the roots were related to the coefficients of the polynomial. It was Viète who gave us symbolic algebra as we recognise it today, though Al-Kwhₐrizmi and even earlier Diophantus, gave us algebra in the written word.

Not much progress on the matter was made until Lagrange's (1736-1813) analysis of resolvent equations, especially in recognising that there were three cube roots of unity, and realising the importance of the permutations of the roots. However his attempts to solve the quintic equation failed. The DFT was first discovered by Carl Friederich Gauss (1777-1855) [1], who also spotted a way of computing the DFT with far fewer than the usual N^2 operations if N was a power of two. That is, he also discovered the Fast Fourier Transform (FFT). Gauss was famous for not publishing, and Joseph Fourier's (1768-1830) researches into heat conduction initiated much research into Fourier series and Fourier transforms which are named in his honour.

Paoli Ruffini (1765-1822) attempted a proof showing it was impossible to solve the general quintic, but there were gaps in the proof. Niels Henrik Abel (1802-1829) independently

proved the impossibility of solving the quintic in terms of radicals, and Abel's proof was water tight, this is now known as the Abel-Ruffini impossibility theorem. (Abel died young due to tuberculosis.) Évariste Galois (1811-1832) further developed the emerging group theory, and was able to show criteria for which quintics were solvable in terms of radicals and which were not. Galois was famously killed by (according to Alexandre Dumas) Pescheux D'Herbinville in a dual over Stéphanie-Felicite Poterin du Motel.

For further reading, we recommend R. Bruce King's "Beyond The Quartic Equation" [2]

References

[1] W. L. Briggs and V. E. Henson, *The DFT: An Owner's Manual for the Discrete Fourier Transform* (SIAM, Philadelphia, 1995).

[2] R. B. King, *Beyond the Quartic Equation* (Modern Birkhauser Classics, Stutgart, Boston, 1996).