The Roots of Early Group Theory in the Works of Lagrange

Janet Heine Barnett*

January 19, 2018

1 Introduction

The problem of solving polynomial equations is nearly as old as mathematics itself. In addition to methods for solving linear equations in ancient India, China, Egypt and Babylonia, solution methods for quadratic equations were known in Babylonia as early as 1700 BCE. Written out entirely in words as a set of directions for calculating a solution from the given numerical values, the Babylonian procedure can easily be translated into a formula which is an early predecessor of today's well-known quadratic formula: $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$, given that $ax^2 + bx + c = 0$. But what about a 'cubic formula' for third degree equations, or a 'quartic formula' for equations of degree four? More generally, is it always possible to compute the solutions of polynomial equations of a given degree by means of a formula based on its coefficients, elementary arithmetic operations and the extraction of roots alone?

As basic as this latter question may sound, its answer eluded mathematicians until the early nineteenth century. In connection with its rather surprising resolution (revealed later in this introduction), there emerged a new and abstract algebraic structure known as a *group*. Algebra, understood prior to that time as the study of solution techniques for equations, was forever changed as a result. In this project, we will explore an example of a particularly important type of group, and will also meet ideas related to a second important type of group, by reading historical excerpts from the earliest phase of the evolution of the group structure. In the remainder of this introduction, we place this reading in context with a brief historical sketch of efforts to find formulas for higher degree polynomial equations.

In a sense, the search for the solution to higher degree polynomials was also pursued by ancient Babylonian mathematicians, whose repertoire included methods for approximating solutions of certain types of cubic equations. The problem of finding exact (versus approximate) solutions might be traced to the somewhat later geometric tradition of ancient Greece, in which there arose problems such as the 'duplication of a cube' (i.e., constructing the side

*Department of Mathematics and Physics; Colorado State University-Pueblo; Pueblo, CO 81001-4901; janet.barnett@csupueblo.edu.

of a cube with twice the volume of a given cube, using only straightedge and compass beginning with the side of the given cube) that correspond to cubic equations when translated into today's algebraic symbolism (i.e., $x^3 = 2$). In order to construct the line segments which served as solutions of the geometrical problems in which they were interested, Greek mathematicians developed various new curves, including the conic sections (i.e., parabolas, hyperbolas and ellipses).[1] Much later, the Islamic mathematician and poet Omar Khayyam (1048–1131) explicitly solved cubic equations by intersecting appropriate conic sections. For example, for a cubic equation of the form $x^3 + d = bx^2$, the points of intersection of the hyperbola $xy = d$ and the parabola $y^2 + dx - db = 0$ correspond to the real roots of the polynomial.[2] Because negative numbers were not allowed as coefficients (or roots) of equations at the time, however, $x^3 + d = bx^2$ was only one of thirteen cubic forms which did not reduce to linear or quadratic equations, each of which required different combinations of conic sections for their solution. Khayyam gave the first systematic classification of all thirteen forms and demonstrated how to solve each geometrically.

Unlike the Greeks, Khayyam and his fellow medieval Islamic mathematicians hoped to find algebraic algorithms for cubic equations — similar to the quadratic formula for second degree equations — in addition to geometric constructions based on curves. Although they were unsuccessful in this regard, it was through Islamic texts that algebra became known in Western Europe. As a result, the search for an algebraic method of solution for higher degree equations was next taken up in Renaissance Italy beginning in the fourteenth century. Some equations studied in this setting were solved through substitutions which reduced the given equation to a quadratic or to a special form like $x^n = a$. Most higher degree equations, however, cannot be solved this way. Only in the sixteenth century, when methods applying to all cubic and quartic polynomials were finally developed, did the Italian search for general solutions achieve some success. The culmination of this search — described in footnote 3 below — is one of the great stories in the history of mathematics.[3]

---

[1]Using abstract algebra, it can now be shown that certain of these construction problems, including the duplication of the cube, are impossible using only the Euclidean tools of a collapsible compass and an unmarked straightedge. Likewise, these ideal Euclidean tools are not sufficient to construct a conic section.

[2]To verify this, substitute $y = \frac{d}{x}$ from the equation of the hyperbola into the equation of the parabola, and simplify. Of course, modern symbolism was not available to Khayyam, who instead wrote out his mathematics entirely in words.

[3]Set in the university world of sixteenth century Italy, where tenure did not exist and faculty appointments were influenced by a scholar's ability to win public challenges, the tale of the discovery of general formulas for cubic and quartic equations begins with Scipione del Ferro (1465–1526), a professor at the University of Bologna. Having discovered a solution method for equations of the form $x^3 + cx = d$, del Ferro guarded his method as a secret until just before his death, when he disclosed it to his student Antonio Maria Fiore (ca. 1506). Although this was only one of thirteen forms which cubic equations could assume, knowing its solution was sufficient to encourage Fiore to challenge Niccolò Tartaglia of Brescia (1499–1557) to a public contest in 1535. Tartaglia, who had been boasting he could solve cubics of the form $x^3 + bx^2 = d$, accepted the challenge and went to work on solving Fiore's form $x^3 + cx = d$. Finding a solution just days before the contest, Tartaglia won the day, but declined the prize of 30 banquets to be prepared by the loser for the winner and his friends. (Poisoning, it seems, was not an unknown occurrence.) Hearing of the victory, the mathematician, physician and gambler Gerolamo Cardano (1501–1576) wrote to Tartaglia seeking permission to publish the method in an arithmetic book. Cardano eventually convinced Tartaglia to share his method, which Tartaglia did in the form of a poem, but only under the condition that Cardano would not publish

Although the solution methods discovered in the sixteenth century are interesting in and of themselves, certain consequences of their discovery were of even greater importance to later developments in mathematics. One such consequence was the discovery of complex numbers, whose eventual acceptance was promoted by the fact that square roots of negative numbers often appear in the course of applying the cubic or quartic formulas to specific equations, only to cancel out and leave only real roots in the end.[4] The increased use of symbolism which characterized Western European algebra in the Renaissance period also had important consequences, including the relative ease with which this symbolism allowed theoretical questions to be asked and answered by mathematicians of subsequent generations. Questions about the number and kind of roots that a polynomial equation possesses, for example, led to the formulation of the Fundamental Theorem of Algebra, the now well-known assertion that an n^{th} degree equation has exactly n roots, counting complex and multiple roots. Algebraic symbolism also allowed questions about the relation between roots and factors to be carefully formulated, thereby leading to discoveries like the Factor Theorem, which states that r is a root of a polynomial if and only if $(x - r)$ is one of its factors.

Despite this progress in understanding the theory of equations, the problem of finding an *algebraic* solution expressible only in terms of the coefficients, elementary arithmetic operations, and extraction of roots for equations of degree higher than four resisted solution until the Norwegian Niels Abel (1802–1829) settled it in a somewhat unexpected way. In a celebrated 1824 pamphlet, Abel proved that a 'quintic formula' for the general fifth degree polynomial is impossible.[5] The same is true for equations of higher degree, making the long search for algebraic solutions to general polynomial equations perhaps seem fruitless. Then, as often happens in mathematics, Abel's 'negative' result produced fruit. Beginning with the central idea of Abel's proof — the concept of a 'permutation' — the French mathematician Évariste Galois (1811–1832) used a concept which he called a 'group of permutations' as a means to classify those equations which are solvable by radicals. Soon after publication of Galois' work, permutation groups in the sense that we know them today[6] appeared as just one example of a more general group concept in the paper *On the theory of groups, as depending on the symbolic equation* $\theta^n = 1$, written by British mathematician Arthur Cayley (1821–1895). Although it drew little attention at the time of its publication, Cayley's paper has since been recognized as the inaugural paper in abstract group theory. By the end of the nineteenth century, group theory was playing a central role in a number of mathematical sub-disciplines, as it continues to do today.

---

the result. Although Cardano did not publish Tartaglia's solution in his arithmetic text, his celebrated 1545 algebra text *Ars Magna* included a cubic equation solution method which Cardano claimed to have found in papers of del Ferro, then 20 years dead. Not long after, a furious Tartaglia was defeated in a public contest by one of Cardano's students, Lodovico Ferrari (1522–1565), who had discovered a solution for equations of degree four. The cubic formula discovered by Tartaglia now bears the name 'Cardano's formula.'

[4]The first detailed discussion of complex numbers and rules for operating with them appeared in Rafael Bombelli's *Algebra* of 1560. Their full acceptance by mathematicians did not occur until much later, however, in the nineteenth century.

[5]The Italian mathematician Paolo Ruffini published this same result in 1799, but his proposed proof contained a gap. Abel, who was not aware of Ruffini's work until 1826, described it as "so complicated that it is very difficult to decide the correctness of his reasoning" (as quoted in [Wussing, 1984, p. 97]).

[6]Galois used the term 'group' in a slightly different way than we do today.

In this project, we will study one of the early precursors of abstract group theory through selections from the writings of the French mathematician J. L. Lagrange (1736–1813). An important figure in the development of group theory, Lagrange made the first real advance in the problem of solving polynomial equations by radicals since the work of Cardano and his sixteenth century contemporaries. In particular, Lagrange was the first to suggest a relation between permutations and the solution of equations by radicals that was later exploited by the mathematicians Abel and Galois. We begin, in Section 2, with an overview of Lagrange's approach to the problem of solving general polynomial equations.

2 Lagrange on the solution of algebraic equations

Born on January 25, 1736 in Turin, Italy to parents of French ancestry, Joseph Louis Lagrange was appointed as a professor of mathematics at the Turin Royal Artillery School by the age of 19. He spent the first eleven years of his professional life teaching there, the next twenty as a mathematical researcher at the Berlin Academy of Sciences, and the final twenty-seven as both a teacher and researcher in Paris, where he died on April 10, 1813. Largely self-taught, he is remembered today for contributions to every branch of eighteenth century mathematics, and especially for his work on the foundations of calculus. His work in algebra is also recognized as sowing one of the seeds that led to the development of group theory in the nineteenth century.

Lagrange's work on the algebraic solution of polynomial equations — that is, a solution expressible only in terms of the coefficients, elementary arithmetic operations and extraction of roots — was first published as a lengthy article entitled 'Réflexions sur la résolution algébrique des équations' in the *Mémoire de l'Académie de Berlin* of 1770 and 1771. As with all his research, generality was Lagrange's primary goal in his works on equations. In seeking a general method of algebraically solving all polynomial equations, he began by looking for the common features of the solutions methods for quadratics, cubics, and quartics. Following a detailed analysis of the known methods of solution, he concluded that one thing they had in common was the existence of an auxiliary (or *resolvent*) equation whose roots (if they could be found) would allow one to easily find the roots of the originally given equation. Furthermore, Lagrange discovered that it was always possible, for any given equation, to find a resolvent equation with roots which are related to the roots of the original equation in a very special way. This special relationship, and a summary of its importance to his work, are nicely described in Lagrange's own words in the following excerpt from his *Traité de la résolution des équations numériques*[7] [Lagrange, 1808].[8]

[7]As suggested by its title, *Traité de la résolution des équations numériques* primarily addressed the problem of numerically approximating solutions to equations; it also included a summary of Lagrange's 1770/1771 work on finding exact solutions to polynomial equations as an appendix entitled 'Note XIII: Sur le résolution des équations algébriques' (see [Lagrange, 1808, pp. 295-327]).

[8]The English translation of this and all other Lagrange excerpts in this project are due to the author.

On the solution of algebraic equations[9]

The solution of second degree equations is found in Diophantus and can also be deduced from several propositions in Euclid's *Data*; but it seems that the first Italian algebraists learned of it from the Arabs. They then solved third and fourth degree equations; but all efforts made since then to push the solution of equations further has accomplished nothing more than finding new methods for the third and the fourth degree, without being able to make a real start on higher degrees, other than for certain particular classes of equations, such as the reciprocal equations, which can always be reduced to a degree less than half [the original degree] ...

In *Mémoire de l'Académie de Berlin* (1770, 1771), I examined and compared the principal methods known for solving algebraic equations, and I found that the methods all reduced, in the final analysis, to the use of a secondary equation called the *resolvent*, for which the roots are of the form

$$x' + \alpha x'' + \alpha^2 x''' + \alpha^3 x^{(iv)} + \dots$$

where $x', x'', x''', \dots$ designate the roots of the proposed equation, and α designates one of the roots of unity, of the same degree as that of the equation.

I next started from this general form of roots, and sought *a priori* for the degree of the resolvent equation and the divisors which it could have, and I gave reasons why this [resolvent] equation, which is always of a degree greater than that of the given equation, can be reduced in the case of equations of the third and the fourth degree and thereby can serve to resolve them.

The rest of this section includes some comments and an example that elaborate on the ideas that Lagrange proposed in this excerpt. Before continuing with your reading, check your understanding of some basic vocabulary by completing the following task.

Task 1 This task reviews some basic vocabulary and mathematical developments discussed in the introduction and the preceding Lagrange excerpt.

(a) What do we mean when we say a polynomial equation is 'algebraically solvable'? Before Lagrange, for which polynomial degrees were algebraic solutions known?

(b) What is a 'resolvent equation'? How does the degree of the resolvent equation compare to the degree of the given equation?

[9] To set them apart from the project narrative, all original source excerpts are set in sans serif font and bracketed by the following symbol at their beginning and end:

Lagrange's emphasis on the *form* of the roots of the resolvent equation is a mark of the more abstract approach he adopted in all his work. Although we will not go through the analysis which led him to identify this form, we will later (in section 4) read through several of the arguments that Lagrange deduced from its existence.[10] Notice for now that the expression for the roots t of the resolvent equation for a polynomial of degree m is actually the sum of only finitely many terms:

$$t = x' + \alpha x'' + \alpha^2 x''' + \alpha^3 x^{(iv)} + \ldots + \alpha^{m-1} x^{(m)}.$$

Lagrange used prime notation ($x', x'', x''', \ldots$) here instead of subscripts ($x_1, x_2, x_3, \ldots$) to denote the m roots of the original equation (and not to indicate derivatives). Similarly, $x^{(m)}$ denotes one of these m roots (and neither a derivative nor a power of x). The symbols $\alpha^2, \alpha^3, \ldots$ here *do* denote powers of α, however, where α itself denotes an m^{th} root of unity: that is, a number for which $\alpha^m = 1$. Of course, $\alpha = 1$ is always a solution of the equation $\alpha^m = 1$. By the Fundamental Theorem of Algebra, however, we know that $\alpha = 1$ is only one of m (possibly distinct) solutions of the equation $\alpha^m = 1$. Letting $i = \sqrt{-1}$, for example, the four fourth roots of unity are $\{1, i, -1, -i\}$.[11] Although Lagrange specified no restrictions on the value which α may assume in the formula for the resolvent's roots in the preceding excerpt, his 1808 summary later made it clear that for $m > 2$, this formula requires α to be a complex-valued root of unity.

Because complex roots of unity played a major role in his analysis, Lagrange included a detailed discussion of their properties in his works on the theory of equations. We will consider excerpts of this discussion — especially those parts which relate to group theory concepts — in Section 3 below. We will also look at methods for computing the values of complex roots of unity in that section. In Section 4, we will then return to the formula Lagrange gave for the roots of the resolvent equation ($t = x' + \alpha x'' + \alpha^2 x''' + \alpha^3 x^{(iv)} + \ldots + \alpha^{m-1} x^{(m)}$), and examine how rearranging (or permuting) the roots $x', x'', x''', \ldots$ within this formula provides us with information about the degree of the resolvent equation.

To set the stage for these discussions, let's first look at a specific example to see how an auxiliary equation, even one of higher degree than the original, can be used to solve a given equation. We note that our primary purpose with this example and its continuation in several later tasks is to provide a context for the group-theoretic connections which emerge from Lagrange's theoretical work on resolvent equations (e.g., roots of unity and permutations), rather than to provide a complete development of that work.

---

[10] As indicated in the excerpt, Lagrange arrived at this expression for the roots of the resolvent equation by examining several specific methods for solving cubics and quartics; that is, his knowledge of this general principle arose from an *a posteriori* analysis of particular instances. An *a priori* analysis, in contrast, is one that starts from a general law and moves to particular instances. The literal meanings of these Latin terms are 'from what comes after' (*a posteriori*) and 'from what comes first' (*a priori*). The arguments we will see below illustrate how Lagrange argued from general algebraic properties in an *a priori* fashion to deduce the degree of the resolvent equation.

[11] This can be verified by solving $(\alpha^2 - 1)(\alpha^2 + 1) = 0$, or by raising each number to the fourth power. As a preview of ideas to come later in this project, note that powers of i give all four roots: $i^1 = i$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$.

A Specific Resolvent Equation Example: Part I

This example is based on Lagrange's analysis [Lagrange, 1770-1771] of the solution given by Gerolamo Cardano (see footnote 3) to the following cubic equation, where $n, p \in \mathbb{R}^+$:

$$x^3 + nx + p = 0, \tag{1}$$

Using basic algebra, it is straightforward to check *(do this!)* that the substitution $x = \frac{t}{3} - \frac{n}{t}$, where $t \neq 0$, transforms the cubic equation (1) into the following sixth degree equation:

$$t^6 + 27pt^3 - 27n^3 = 0 \tag{2}$$

In Lagrange's terminology, equation (2) is a **resolvent equation** for the given cubic equation (1). This means we can find the three roots of the given cubic equation (1) using only elementary arithmetic operations and extraction of roots involving the given coefficients $(1, n, p)$, by first finding the six roots of the resolvent equation (2). Here's how:

(i) Notice that the resolvent equation (2) is quadratic in t^3: $\quad [t^3]^2 + 27p\,[t^3] - 27n^3 = 0.$

The quadratic formula gives us the roots of $\theta^2 + 27p\theta - 27n^3$ in the required algebraic form. Denote these two roots as θ_1 and θ_2.
Because n and p are positive reals, it's easy to check that θ_1, θ_2 are distinct real numbers.[a]
It follows that $t_1 = \sqrt[3]{\theta_1}$ and $t_2 = \sqrt[3]{\theta_2}$ are distinct real roots of the resolvent equation, and also that t_1, t_2 are expressed in the required form. *(Do you see why?)*

(ii) Lagrange then showed that the remaining four (complex) roots of the resolvent equation (2) can be written in the required algebraic form, by first writing each of these four (complex) roots as products involving t_1, t_2 and the two complex-valued cubic roots of unity.[b]

For instance, letting α denote a complex number with $\alpha^3 = 1$,
the following computation shows that $t_3 = \alpha t_1$ is also root of the resolvent equation:

$$\begin{array}{lcll} (\alpha t_1)^6 + 27p(\alpha t_1)^3 - 27n^3 & = & \alpha^6 t_1^6 + 27p\alpha^3 t_1^3 - 27n^3 & \text{by basic algebra} \\ & = & t_1^6 + 27pt_1^3 - 27n^3 & \text{since } \alpha^3 = 1,\ \alpha^6 = (\alpha^3)^2 = 1 \\ & = & 0 & \text{since } t_1 \text{ is a root of the resolvent} \end{array}$$

Letting α, β denote the two complex cubic roots of unity, the remaining roots of the resolvent equation can then be similarly obtained by setting $t_4 = \beta t_1$, $t_5 = \alpha t_2$ and $t_6 = \beta t_2$.

(iii) Now that every solution t of the resolvent equation is expressed in the required algebraic form, the substitution $x = \frac{t}{3} - \frac{n}{t}$ gives the three solutions of the original cubic equation in that same required form; that is, using only elementary arithmetic operations and the extraction of roots beginning from the coefficients $(1, n, p)$ of the given cubic.

---

[a] One way to check that θ_1, θ_2 are distinct real numbers is to show that the discriminant $b^2 - 4ac = 27^2p^2 + 4(27n^3)$ is strictly positive. Can you think of other ways to do this?

[b] We could also express the four complex roots of the resolvent directly in terms of i and the roots θ_1, θ_2 of the quadratic $\theta^2 + 27pt^3 - 27n^3$ by using the substitution $\theta = t^3$ to first rewrite the resolvent equation as follows:

$$\begin{array}{rcl} t^6 + 27pt^3 - 27n^3 & = & (t^3 - \theta_1)(t^3 - \theta_2) \ = \ (t^3 - (\sqrt[3]{\theta_1})^3)(t^3 - (\sqrt[3]{\theta_2})^3) \\ & = & (t - \sqrt[3]{\theta_1})(t^2 + \sqrt[3]{\theta_1}t + \sqrt[3]{\theta_1}^2)(t - \sqrt[3]{\theta_2})(t^2 + \sqrt[3]{\theta_2}t + \sqrt[3]{\theta_2}^2) \end{array}$$

Applying the quadratic formula to the quadratic factors then gives the resolvent roots in the required algebraic form.

As you read the example on the preceding page, did you wonder how the six roots of the resolvent equation give us only three roots for the original cubic? Here's how this works for the real-valued roots.

- Begin by setting $x_1 = \frac{t_1}{3} - \frac{n}{t_1}$ and $x_2 = \frac{t_2}{3} - \frac{n}{t_2}$, and remember that $t_1 = \sqrt[3]{\theta_1}$ and $t_2 = \sqrt[3]{\theta_2}$, where θ_1 and θ_2 denote the two real-valued roots of the quadratic function $\boxed{f(\theta) = \theta^2 + 27p\theta - 27n^3}$.
- By the Factor Theorem, we know that $f(\theta) = (\theta - \theta_1)(\theta - \theta_2)$. Expand this to get $\boxed{f(\theta) = \theta^2 - (\theta_1 + \theta_2)\theta + \theta_1\theta_2}$.
- Since the two boxed expressions above represent the same quadratic function, the coefficients must be the same. Equating the constant coefficient gives us $\theta_1\theta_2 = (-3n)^3$.
- Since $\theta_1 = t_1^3$ and $\theta_2 = t_2^3$, it follows that $t_1t_2 = -3n$, or $3n = -t_1t_2$.
- Substituting this last fact in the defining expression for x_1, we have:

$$x_1 = \frac{t_1}{3} - \frac{n}{t_1} = \frac{t_1}{3} - \frac{3n}{3t_1} = \frac{t_1}{3} - \frac{(-t_1t_2)}{3t_1} = \frac{1}{3}(t_1 + t_2).$$

- Proceeding similarly *(do this!)*, we can show that $x_2 = \frac{1}{3}(t_1 + t_2)$, so that $x_1 = x_2$!

Analogous computations with the 2-to-1 function $x(t) = \frac{t}{3} - \frac{n}{t}$ will show that $x_3 = x_6$ and $x_4 = x_5$. We will look at the complex computations associated with these two equalities in Section 3, after first briefly studying the properties of complex roots of unity.

3 Roots of unity in Lagrange's analysis

As suggested above, roots of unity played an important role in Lagrange's formula for the roots of the resolvent equation, and more generally in the theory of equations. In this section, we consider some properties of these special roots as they were described by Lagrange.

Our first excerpt on roots of unity also touches on an important point about 'solvability' which we have already raised; namely, the notion of 'solvability' can be defined in a variety of ways. We know from the introduction, for example, that Omar Khayyam continued to seek an algebraic algorithm for the roots of cubic equations, even after he showed these roots existed by intersecting conic sections in a way that would have satisfied Greek mathematicians as a legitimate solution. In our context, 'algebraic solvability' also specifically requires that the roots of a given equation can be determined from its coefficients by way of a *finite* number of steps involving only elementary arithmetic operations $(+, -, \times, \div)$ and the extraction of roots. The solution involving trigonometric functions described below by Lagrange would thus not count as an algebraic solution for today's algebraist (nor would it for Lagrange) *unless* the specific trigonometric values involved could be expressed in the permitted form. We examine this issue further in the following excerpt, taken from Note XIV of Lagrange's *Traité de la résolution des équations numériques* [Lagrange, 1808].

Although equations with two terms such as

$$x^m - A = 0, \text{or more simply } x^m - 1 = 0$$

(since the former is always reducible to the latter, by putting $x\sqrt[m]{A}$ in for x), are always solvable by trigonometric tables in a manner that allows one to approximate the roots as closely as desired, by employing the known formula[12]

$$x = \cos\frac{k}{m}360^\circ + \sin\frac{k}{m}360^\circ\sqrt{-1}$$

and letting $k = 1, 2, 3, \ldots, m$ successively, their algebraic solution is no less interesting for Analysis, and mathematicians have greatly occupied themselves with it.

Today, this trigonometric formula for the m^{th} roots of unity is written in terms of the radian measure of a circle, 2π, and the now-standard symbol $i = \sqrt{-1}$:

$$x^m - 1 = 0 \quad \Leftrightarrow \quad x = \cos\left(\frac{2\pi k}{m}\right) + i\sin\left(\frac{2\pi k}{m}\right), \text{ where } k = 1, 2, 3, \ldots, m.$$

For example, the solutions of $x^3 - 1 = 0$ are readily obtained from this formula as follows:

$$\begin{array}{rcccccc} k=1 & \Rightarrow & x = \cos\left(\frac{2\pi\cdot 1}{3}\right) + i\sin\left(\frac{2\pi\cdot 1}{3}\right) & = & \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right) & = & -\frac{1}{2} + \frac{\sqrt{3}}{2}i \\ k=2 & \Rightarrow & x = \cos\left(\frac{2\pi\cdot 2}{3}\right) + i\sin\left(\frac{2\pi\cdot 2}{3}\right) & = & \cos\left(\frac{4\pi}{3}\right) + i\sin\left(\frac{4\pi}{3}\right) & = & -\frac{1}{2} - \frac{\sqrt{3}}{2}i \\ k=3 & \Rightarrow & x = \cos\left(\frac{2\pi\cdot 3}{3}\right) + i\sin\left(\frac{2\pi\cdot 3}{3}\right) & = & \cos(2\pi) + i\sin(2\pi) & = & 1 \end{array}$$

Notice that these roots include one real root and two complex roots which are conjugates of each other. Also note that the particular trigonometric values involved here can be expressed in terms of only finitely many basic arithmetic operations on rational numbers and their roots (including $i = \sqrt{-1}$).[13] In fact, we could instead solve $x^3 - 1 = 0$ by first factoring $[x^3 - 1 = (x-1)(x^2 + x + 1)]$ and then using the quadratic formula. Thus, the cubic roots of unity are bona fide algebraic solutions of this equation.

In his celebrated doctoral dissertation *Disquisitiones Arithmetica* of 1801, the great German mathematician Frederic Gauss (1777–1855) proved that $x^m - 1 = 0$ can always be solved algebraically. This fact in turn implied Lagrange could legitimately use roots of unity in his formula for the roots of the resolvent and still obtain an algebraic solution. Lagrange commented on this technical point in his 1808 summary, saying of Gauss' work that it was 'as original as it was ingenious' [Lagrange, 1808, p. 329].

[12] A proof of this formula lies outside the scope of this project.

[13] Had the coefficients of the original equation included irrational or imaginary numbers, then any number obtained in a finite number of steps from those coefficients with basic arithmetic operations or extraction of roots would also be allowed. Since the coefficients of $x^3 - 1 = 0$ are integers, these operations allow only rational numbers and their roots.

Task 2 Without employing a calculator or computer, use the formula $x = \cos\left(\frac{2\pi k}{m}\right) + i \sin\left(\frac{2\pi k}{m}\right)$ (with $m = 6$) to express all sixth roots of unity in terms of the elementary arithmetic operations on rational numbers and their roots only.

What difficulties do we encounter when we try to do this for the **fifth** roots of unity?[14]

As Lagrange commented, the formula stated in the preceding excerpt for expressing the m^{th} roots of unity in terms of the trigonometric functions was well-known by his time. It is straightforward to check the correctness of this formula (see Appendix II, Task I) using another formula that was then well-known:

de Moivre's Formula: $(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$

The mathematician for which this formula is named, Abraham de Moivre[15] (1667–1754), appears to have had some understanding of it as early as 1707, but never published a proof. In the first-ever published precalculus text, *Introductio in analysin infinitorum* (1748), the celebrated mathematician Leonhard Euler (1707–1783) used standard trigonometric identities to prove de Moivre's formula in the case where n is a natural number (see Appendix II, Task II). As was typical of Euler, he then took matters further and used power series (see Appendix II, Task III) to establish another amazing formula:

Euler's formula: $e^{i\theta} = \cos\theta + i\sin\theta$

As a corollary to Euler's formula, de Moivre's formula is easy to prove, although the almost magical ease of this proof makes it seem no less mysterious:[16]

$$(\cos\theta + i\sin\theta)^n = (e^{i\theta})^n = e^{i(n\theta)} = \cos(n\theta) + i\sin(n\theta)$$

Additionally, Euler's formula gives us another (more concise) way to represent roots of unity:

$$x^m - 1 = 0 \quad \Leftrightarrow \quad x = \cos\left(\frac{2\pi k}{m}\right) + i\sin\left(\frac{2\pi k}{m}\right) \quad \Leftrightarrow \quad x = e^{\frac{2\pi k}{m}i}, \text{ where } k = 1, 2, 3, \ldots, m.$$

Although Lagrange himself did not make use of this exponential representation in his own writing (despite his familiarity with Euler's identity), we will use it as a convenient notational abbreviation and to simplify computations. For example, the three cubic roots of unity can be written as follows:

---

[14] Lagrange found the values of the fifth roots of unity to be 1, $\frac{\sqrt{5}-1}{4} \pm \frac{\sqrt{10+2\sqrt{5}}}{4}i$, and $-\frac{\sqrt{5}+1}{4} \pm \frac{\sqrt{10-2\sqrt{5}}}{4}i$ — but not by using trigonometric functions! See Appendix I for a sketch of one of the approaches that he used for deriving these values.

[15] Although born in France, de Moivre lived as an exile in England for most of his life as the result of severe religious persecution of Protestants in France following the issue of the Edict of Fontainebleau in 1685.

[16] Another easy but mysterious consequence of Euler's formula, obtained by letting $\theta = \pi$, is **Euler's Identity** relating the five most important mathematical constants in a single equation: $e^{i\pi} + 1 = 0$. After proving Euler's identity to an undergraduate class at Harvard, the American algebraist Benjamin Peirce (1809–1880) is reported in [Archibald, 1925] to have said: "Gentlemen, that is surely true, it is absolutely paradoxical; we cannot understand it, and we don't know what it means. But we have proved it, and therefore we know it must be the truth."

$$
\begin{aligned}
k = 1 \quad &\Rightarrow \quad x = e^{\frac{2\pi \cdot 1}{3} i} = e^{\frac{2\pi i}{3}} \\
k = 2 \quad &\Rightarrow \quad x = e^{\frac{2\pi \cdot 2}{3} i} = e^{\frac{4\pi i}{3}} \\
k = 3 \quad &\Rightarrow \quad x = e^{\frac{2\pi \cdot 3}{3} i} = e^{2\pi i}
\end{aligned}
$$

We also make use of the geometric representation of roots of unity as points on the unit circle (see Figure 1) which is naturally suggested by the formula $e^{\frac{2\pi k}{m} i} = \cos\left(\frac{2\pi k}{m}\right) + i \sin\left(\frac{2\pi k}{m}\right)$.

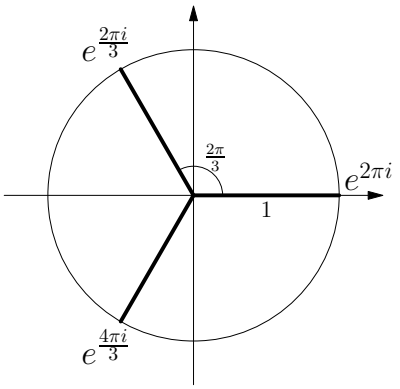


Figure 1: Cubic roots of unity: $e^{\frac{2\pi k}{3} i} = \cos\left(\frac{2\pi k}{3}\right) + i \sin\left(\frac{2\pi k}{3}\right)$, $k = 1, 2, 3$

Task 3

(a) Represent the sixth roots of unity on a unit circle. (See also Task 2.)
Label these in exponential form: $e^{\frac{2\pi k}{6} i} = e^{\frac{\pi k}{3} i}$, where $k = 1, 2, 3, 4, 5, 6$.
Also indicate clearly which of these six roots are real and which are complex.

(b) On the unit circle from part (a), identify which of the sixth roots of unity are also square roots of unity, and which are also cubic roots of unity.

(c) Use a separate unit circle to represent the fifth roots of unity; again label with exponential notation and indicate which are real and which are complex.

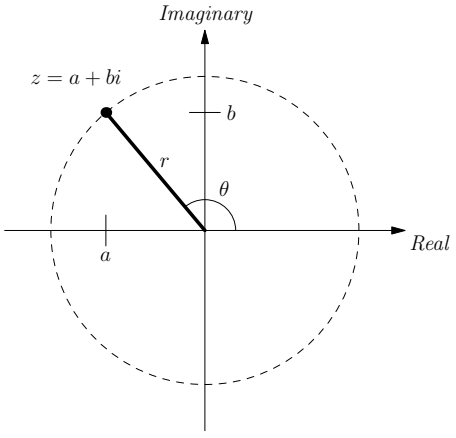
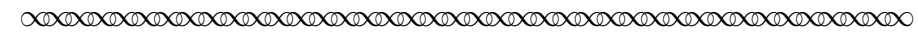


Figure 2: Geometric representation of $z = a + bi = re^{i\theta}$, where $r = \sqrt{a^2 + b^2}$

Although the geometric representation of the set of all complex numbers as points in the two-dimensional plane shown in Figure 2 was first published after Lagrange's work on

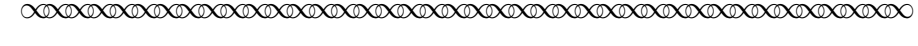
algebraic solvability,[17] mathematicians of his era were well aware of the connection of roots of unity to the unit circle.[18] In fact, Lagrange explicitly used the geometric representation of roots of unity as points on the unit circle to determine the total number and type (real versus complex) of m^{th} roots of unity, as we read in the following excerpt from his 1770 *Mémoire*.[19] It may be helpful to refer back to the unit circles in Figure 1 and Task 3 as you read this excerpt.



We first remark concerning this solution that each of the roots of the equation $x^m - 1 = 0$ should be different from each other, since on the circumference there are not two different arcs which simultaneously have the same sine and the same cosine. It is further easy to see that all the roots will be imaginary, with the exception of the last which corresponds to $k = m$ and which will always equal 1, and of that which corresponds to $k = \frac{m}{2}$, when m is even, which will equal -1; since in order for the imaginary part of the expression of x to vanish, it is necessary to have

$$\sin\left(\frac{k}{m}360^\circ\right) = 0,$$

which never occurs unless the arc is equal to 360° or to 180°; in which case we will have either $\frac{k}{m} = 1$ or $= \frac{1}{2}$, and consequently either $k = m$ or $k = \frac{m}{2}$; in the first case, the real part $\cos\left(\frac{k}{m}360^\circ\right)$ will become $\cos 360^\circ = 1$; and in the second it will become $\cos 180^\circ = -1$.



Task 4 Compare Lagrange's claim concerning the number and type of m^{th} roots of unity in the preceding excerpt to what you found for $m = 6$ in parts (a) and (b) of Task 3.

How convincing do you find Lagrange's argument in general?

We now read the continuation of Lagrange's comments on roots of unity, in which ideas related to what later came to be known as a 'cyclic group' arise for the first (but not last!) time in this project.

[17] The name of Parisian bookkeeper Jean-Robert Argand (1768–1822) is frequently cited in connection with the development of the complex plane, in recognition of an 1806 pamphlet which he produced on the topic. Although there are indications that Gauss was in possession of the geometric representation of complex numbers as early as 1796, he did not publish on the subject until 1831. Credit for the first publication on the subject instead belongs to the Norwegian Caspar Wessel (1745–1818); unfortunately, Wessel's 1797 paper was written in Danish and went unnoticed until 1897.

[18] It was this relation of the m^{th} roots of unity to points on the unit circle that led to the term 'cyclotomic polynomial' being used for the expression '$x^{m-1} + x^{m-2} + \ldots + 1$' which arises as a factor of $x^m - 1 = (x-1)(x^{m-1} + x^{m-2} + \ldots + 1)$.

[19] Because the following excerpt comes from a different source than that which we have quoted thus far, we have altered the notation in it slightly (replacing, for example, n by m) to be consistent with the notation used in our other excerpts.

Now, if we let

$$\alpha = \cos\left(\frac{360^\circ}{m}\right) + \sin\left(\frac{360^\circ}{m}\right)\sqrt{-1},$$

we will have ...

$$\alpha^k = \cos\left(\frac{k}{m}360^\circ\right) + \sin\left(\frac{k}{m}360^\circ\right)\sqrt{-1};$$

so that the different roots of $x^m - 1 = 0$ will all be expressed by the powers of this quantity α; and thus these roots will be $\alpha, \alpha^2, \alpha^3, \ldots \alpha^m$, of which the last α^m will always be equal to 1 ....

We pause at this point in our reading of Lagrange to illustrate his central idea for the specific case of $m = 3$. Using exponential notation, we set $\alpha = e^{\frac{2\pi i}{3}}$. Then, as noted by Lagrange, the remaining cubic roots of unity can be obtained simply by taking powers of α, since $\alpha^2 = \left[e^{\frac{2\pi i}{3}}\right]^2 = e^{\frac{4\pi i}{3}}$ and $\alpha^3 = \left[e^{\frac{2\pi i}{3}}\right]^3 = e^{2\pi i} = 1$. Because it is possible to generate all the cubic roots of unity from α in this way, α is called a ***primitive cubic root of unity***.

Task 5 Let $m = 6$ and set $\alpha = \cos\left(\frac{2\pi}{6}\right) + i\sin\left(\frac{2\pi}{6}\right) = e^{\frac{\pi i}{3}}$.
Verify that α is a primitive sixth root of unity by computing α^k for $k = 2, 3, 4, 5, 6$.
Comment on how these results compare to your answer to Task 3(a).

We return now to Lagrange's comments on primitive roots of unity.

It is good to observe here that if m is a prime number, one can always represent all the roots of $x^m - 1 = 0$ by the successive powers of any one of these same roots, excepting only the last; let, for example, $m = 3$, the roots will be $\alpha, \alpha^2, \alpha^3$: if we take the next root α^2 in place of α, we have the three roots $\alpha^2, \alpha^4, \alpha^6$; but, since $\alpha^3 = 1$, it is clear that $\alpha^4 = \alpha$ and that $\alpha^6 = \alpha^3$; so that these roots will be $\alpha^2, \alpha, \alpha^3$, the same as before.

Let us consider what Lagrange is claiming here in more detail. In light of his comments on primitive roots of unity in the first excerpt on the preceding page, we know the expression 'the last root' is a reference to the real number '1', obtained by taking the 'last' power (α^m) of $\alpha = e^{\frac{2\pi i}{m}}$. We also know from what Lagrange has already said that $\alpha = e^{\frac{2\pi i}{m}}$ is a primitive m^{th} root of unity, since taking powers of α has the effect of cycling through all the m^{th} roots of unity. In the excerpt we have just read, Lagrange has gone beyond this to claim that *every* m^{th} root of unity — other than the last root 1 — behaves in exactly this same way, provided m is prime. In other words, Lagrange has asserted the following theorem:

Theorem
If $m \in \mathbb{Z}^+$ is prime and β is an m^{th} root of unity with $\beta \neq 1$,
then β is a primitive m^{th} root of unity.

Lagrange's illustration of this theorem for the prime $m = 3$ in the preceding excerpt used the fact that $\alpha = e^{\frac{2\pi i}{3}}$ is already known to be a primitive cubic root of unity; thus, the only other complex root of unity β can be written as a power of α; namely, $\beta = \alpha^2$. Using this notation, we can re-write Lagrange's power computations as follows: $\beta^1 = \alpha^2$, $\beta^2 = \alpha^4 = \alpha^3\alpha = \alpha$ and $\beta^3 = \alpha^6 = [\alpha^3]^2 = 1$. This shows that $\beta = \alpha^2$ is also a primitive root of unity, and the theorem holds in this case.

Task 6 Following his discussion of cubic roots of unity in the preceding excerpt, Lagrange next considered the case $m = 5$, where $\alpha = \cos\left(\frac{2\pi}{5}\right) + i\sin\left(\frac{2\pi}{5}\right) = e^{\frac{2\pi i}{5}}$ and the five fifth roots of unity are $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5 = 1$.

Complete the following to prove that α^2, α^3, and α^4 are also primitive fifth root of unity.

(a) Find the first five powers of α^2, and show that these are the same as the five original roots rearranged in the following order: $\alpha^2, \alpha^4, \alpha, \alpha^3, \alpha^5$

(b) Find the first five powers of α^3, and show that these generate the five original roots rearranged in the following order: $\alpha^3, \alpha, \alpha^4, \alpha^2, \alpha^5$.

(c) Determine the order in which the original roots are generated using powers of α^4.

In the next task, the specific case of $m = 6$ is used to show that the restriction to prime numbers in the preceding theorem is necessary; that is, when m is composite, it is no longer the case that every complex root of unity is also a primitive root of unity. A proof of the theorem for the prime case is then outlined in Task 8, followed by further explorations of the composite case in Task 9.

Before turning to these tasks, we introduce some current notation and terminology that will be convenient to use in the rest of this section. Given $m \in \mathbb{Z}^+$, let's denote the set of all m^{th} roots of unity as:

$$U_m = \{x \in \mathbb{C} | x^m = 1\} = \{e^{\frac{2k\pi}{m}i} | k = 1, 2, \ldots, m\}$$

Given any root of unity β, we will also write

$$\langle \beta \rangle = \{\beta^n | n \in \mathbb{Z}\},$$

where the set $\langle \beta \rangle$ is called either the **set generated by** β, or the **group generated by** β. Using this terminology and notation for the results from Task 6c, for instance, we can write the group generated by α^4 (where $\alpha = e^{\frac{2\pi}{5}i}$) as:

$$\langle \alpha^4 \rangle = \{\, \alpha^4 \,,\, \alpha^3 \,,\, \alpha^2 \,,\, \alpha \,,\, \alpha^5 \,\} = U_5$$

Notice that, since $\langle \alpha^4 \rangle = U_5$, we can conclude that α^4 is a primitive fifth root of unity. Similarly, in the general case, β is a *primitive* root of unity iff $\langle \beta \rangle = U_m$. When this occurs, we will also say that β **generates** U_m, or that β **is generator of** U_m.

Task 7 In this task, the case $m = 6$ is used to show that the restriction to prime numbers in the preceding theorem is necessary; that is, when m is composite, it is no longer the case that *every* root of unity can be used to generate all m roots of unity via powers.

Set $\alpha = \cos\left(\frac{2\pi}{6}\right) + i \sin\left(\frac{2\pi}{6}\right) = e^{\frac{\pi}{3}i}$.

(a) Explain why all the sixth roots of unity are obtained by taking powers of α.
That is, show that $\langle \alpha \rangle = U_6$.
(It may be useful to review the unit circle diagram from Task 3, parts (a) and (b).)

(b) Now find $\langle \alpha^2 \rangle$ by taking powers of $\beta = \alpha^2$.
Which of the sixth roots of unity do you obtain in this case?

(c) Now find $\langle \alpha^3 \rangle$ by taking powers of $\gamma = \alpha^3$.
Which of the sixth roots of unity do you obtain in this case?

(d) Which of the powers of α, other than $\alpha^1 = \alpha$, are also primitive roots of unity? That is, which powers of α generate all six of the sixth roots of unity? Justify your response.

Task 8 In this task, we return to the case where m is prime, and sketch a general proof for Lagrange's claim that every complex m^{th} root of unity β except $\beta = 1$ is primitive.

Begin by assuming that m is prime and that $\beta \neq 1$ is a complex m^{th} root of unity. Also let $\alpha = e^{\frac{2\pi i}{m}}$, and choose $n \in \mathbb{Z}^+$ such that $\beta = \alpha^n$ with $1 \leq n < m$, where $\mathbb{Z}^+$ denotes the set of positive integers. *(How do we know that such a value of n exists?)*

Our goal is to prove that the powers of β generate all possible m^{th} root of unity by proving that $\langle \beta \rangle = U_m$. In other words, we wish to show that the list $\beta\,,\, \beta^2\,,\, \ldots\,,\, \beta^m$ consisting of the first m positive integer powers of β corresponds to some arrangement of the list $\alpha\,,\, \alpha^2\,,\, \ldots\,,\, \alpha^m$ of all m^{th} roots of unity.

(a) Begin by explaining why β^s is an m^{th} root of unity for all $s \in \mathbb{Z}^+$ with $1 \leq s \leq m$.

Note:
Since different powers of β could produce the same complex number, this proves only that the list $\beta\,,\, \beta^2\,,\, \ldots\,,\, \beta^m$ contains *at most* m distinct m^{th} roots of unity.

(b) Use the fact that m is prime to prove the following:

> **Lemma** Assume $m, n \in \mathbb{Z}^+$ with m prime, $\alpha = e^{\frac{2\pi i}{m}}$, and $\beta = \alpha^n$.
> For all $s \in \mathbb{Z}^+$, $\beta^s = 1$ if and only if m divides s.

Hint? Remember that $\alpha = e^{\frac{2\pi i}{m}} = \cos\left(\frac{2\pi}{m}\right) + i \sin\left(\frac{2\pi}{m}\right)$.

Note:
This shows that m is the first positive power of β that generates 'the last root' 1; that is, the real root $1 = \beta^m$ appears only once within the list $\beta\,,\, \beta^2\,,\, \ldots\,,\, \beta^m$.
It remains to show that no other m^{th} roots of unity are repeated in this list.

(c) Suppose that the list $\beta\,,\, \beta^2\,,\, \ldots\,,\, \beta^m$ contains fewer than m distinct values. That is, suppose that $\beta^k = \beta^l$ for some integers k, l with $1 \leq k < l \leq m$.
Use the lemma proven in part (b) to derive a contradiction.
Hint? Notice that $1 \leq l - k < m$.

(d) *Optional:* Re-write the proof that there are no repeated elements in the list $\beta\,,\, \beta^2\,,\, \ldots\,,\, \beta^m$ from part (c) without using proof by contradiction.

Task 9 We now return to the case where m is a composite number and consider the number of primitive m^{th} roots of unity in this case. To this end, let $\alpha = e^{\frac{2\pi}{m}i}$.

(a) Recall that for $m = 4$, the primitive fourth roots of unity are $\alpha = i$ and $\alpha^3 = -i$.
Also review the results which you obtained in Task 7 for the case $m = 6$.
Use this data to develop a general conjecture concerning exactly which powers of α are primitive roots and which are not in the case where m is composite.

(b) Test your conjecture from part (a) in the cases of $m = 8$ and $m = 9$.
Clearly record your evidence that α^s is or is not a primitive root for each value of s.
Refine your conjecture as needed before testing it for the case of $m = 12$.
Continue to refine and re-test it further as needed.
Once you are satisfied with your conjecture, write a general proof for it.
Discuss proof strategies as needed with other students or your course instructor.

(c) *Optional:* Modify your conjecture for primitive roots of unity in the case where m is composite so that it applies to all values of m, both prime and composite.
Also modify your proof as needed to apply to this more general conjecture.

We close this section with a continuation of the specific resolvent equation example from the end of Section 2. In Section 4, we will return to this example once more, and use the expressions obtained for x', x'', x''' below to establish that the special relationship $t = x' + \alpha x'' + \alpha^2 x'''$ which Lagrange claimed will hold between the roots of an equation (x, x', x'') and the roots of its resolvent (t) does indeed hold in this particular example.

A Specific Resolvent Equation Example: Part II

Recall that the roots of the cubic equation $x^3 + nx + p = 0$, where $n, p \in \mathbb{R}^+$, are related to the roots of the sixth degree resolvent equation $t^6 + 27pt^3 - 27n^3 = 0$ by the expression $x = \frac{t}{3} - \frac{n}{t}$.

Also recall that the six (distinct) roots $t_1, t_2, t_3, t_4, t_4, t_6$ of this resolvent equation can be expressed as products of its two real roots (t_1, t_2) and the cubic roots of unity. For example, denoting the cubic roots of unity by $1, \alpha, \alpha^2$, where α is a primitive cubic root of unity, and letting θ_1, θ_2 denote the two (distinct) real roots of $\theta^2 + 27p\theta - 27n^3$, we obtain:

$$\begin{array}{lll} t_1 = \sqrt[3]{\theta_1} & t_3 = \alpha t_1 & t_5 = \alpha^2 t_1 \\ t_2 = \sqrt[3]{\theta_2} & t_4 = \alpha t_2 & t_6 = \alpha^2 t_2, \end{array}$$

Further recall that we can use the fact that $t_1 t_2 = -3n$ to show that $\frac{t_1}{3} - \frac{n}{t_1} = \frac{1}{3}(t_1 + t_2) = \frac{t_2}{3} - \frac{n}{t_2}$, concluding that $x' = \frac{1}{3}(t_1 + t_2)$ is the only real root of the given cubic equation.
Using this same fact $[t_1 t_2 = -3n]$, we see that $t_4 t_5 = (\alpha^2 t_1)(\alpha t_2) = t_1 t_2 = -3n$, which in turn implies:

$$x_4 = \frac{t_4}{3} - \frac{n}{t_4} = \frac{t_4}{3} - \frac{3n}{3t_4} = \frac{t_4}{3} - \frac{(-t_4 t_5)}{3t_4} = \frac{1}{3}(t_4 + t_5) = \frac{t_5}{3} - \frac{(-t_4 t_5)}{3t_6} = \frac{t_5}{3} - \frac{3n}{3t_5} = \frac{t_5}{3} - \frac{n}{t_5} = x_5$$

This shows that $x'' = \frac{1}{3}(t_4 + t_5)$ is one of the two complex roots of the given cubic.

Denoting the second complex root of the given cubic by x''', a similar computation will show that $x''' = \frac{1}{3}(t_3 + t_6)$. *(Be sure to check this!)*

4 Permutations of roots in Lagrange's analysis

We now return to Lagrange's treatment of general polynomial equations in his 1808 note on this topic. The first excerpt we consider states a relationship between the roots and the coefficients of an equation which was well known to algebraists of his time; following the excerpt, we will see how this relationship leads to the idea of permuting roots.

We represent the proposed equation by the general formula

$$x^m - Ax^{m-1} + Bx^{m-2} - Cx^{m-3} + \ldots = 0,$$

and we designate its m roots by $x', x'', x''', \ldots, x^{(m)}$; we will then have, by the known properties of equations,

$$\begin{aligned} A &= x' + x'' + x''' + \ldots + x^{(m)}, \\ B &= x'x'' + x'x''' + \ldots + x''x''' + \ldots, \\ C &= x'x''x''' + \ldots \end{aligned}$$

Task 10

(a) For $m = 2$, note that the general equation becomes $x^2 - Ax + B = 0$, where Lagrange claimed that $A = x' + x''$ and $B = x'x''$. Verify that these formulas for A and B are correct by expanding the polynomial: $(x - x')(x - x'')$.

(b) Now write down the formulas for the coefficients A, B,C of the cubic polynomial $x^3 - Ax^2 + Bx - C$ in terms of its roots x', x'', x''', and again verify that these are correct by expanding the factored form of the polynomial.

(c) Use the formulas found in part (b) for the coefficients A, B, C of the cubic polynomial $x^3 - Ax^2 + Bx - C$ to determine the expanded form of the following polynomials *without* multiplying out the given factors.

(i) $(x - 2)(x - 3)(x - 5)$ **(ii)** $(x - 1)(x - (1 + 2i))(x - (1 - 2i))$

In Lagrange's expressions for the coefficients A, B, C, ..., note that the roots x', x'', x''', ... , $x^{(m)}$ can be permuted in any way we wish without changing the (formal) value of the expression. For example, if we exchange x' for x'' (and vice-versa) in the case where $m = 2$, we get $A = x'' + x'$ and $B = x''x'$, both clearly equal to the original expressions ($A = x' + x''$ and $B = x'x''$). For $m = 3$, more complicated permutations of the roots arise. For example, we could simultaneously replace each occurrence of x' by x''', each occurrence of x'' by x' and each occurrence of x''' by x'' in the original expressions for A, B, C to obtain:

$$\begin{aligned} A = x' + x'' + x''' \quad &\Rightarrow \quad A = x''' + x' + x'' \\ B = x'x'' + x'x''' + x''x''' \quad &\Rightarrow \quad B = x'''x' + x'''x'' + x'x'' \\ C = x'x''x''' \quad &\Rightarrow \quad C = x'''x'x'' \end{aligned}$$

Again we see that the expressions resulting from this particular permutation of the given roots are formally equivalent to the original expressions. It is similarly straightforward to check that this occurs with every possible permutation of the three roots. *(Try it!)*

Expressions with the property that every permutation of the variables results in the same formal value are said to be ***symmetric functions***.[20] In contrast, the expression $x_1x_2 + x_3$ is *not* a symmetric function since, for example, exchanging x_1 and x_3 results in a different formal value $(x_3x_2 + x_1)$, even though exchanging x_1 and x_2 results in an expression $(x_2x_1 + x_3)$ equivalent to the original $(x_1x_2 + x_3)$.

Task 11 Determine which of the following are symmetric expressions in x_1, x_2, x_3.

For any that is not, describe a permutation of x_1, x_2, x_3 that changes the formal expression, and (if possible) another permutation that does not change the formal expression.

(a) $(x_1 + x_2 + x_3)^2$ **(b)** $x_1^2 + (x_2 + x_3)^2$ **(c)** $(x_1 + x_2)(x_2 + x_3)$

Returning now to Lagrange, we read two suggestions concerning how one might proceed to find the resolvent equation whose solution would allow us to find an algebraic solution of the original equation.

> To obtain the [resolvent] equation ..., it will be necessary to eliminate the m unknowns x' ,x'' , x''', ... , $x^{(m)}$ by means of the preceding equations, which are also m in number; but this process requires long calculations, and it will have, moreover, the inconvenience of arriving at a final equation of degree higher than it needs to be.
>
> One can obtain the equation in question directly and in a simpler fashion, by employing a method which we have made frequent use of here, which consists in first finding the form of all the roots of the equation sought, and then composing this equation by means of its roots.

In other words, we can try to write a resolvent equation either by working with m (non-linear) equations in m unknowns through a series of long calculations involving symmetric functions ... or we can simplify this process by using the *form* of the roots to obtain the resolvent equation by way the Factor Theorem, with each root contributing a factor towards building up the resolvent equation.

In our remaining excerpts from Lagrange's work, we will see how he set out to implement this second plan. The tasks interspersed between these excerpts examine his argument in the specific case $m = 3$. We begin with an excerpt in which Lagrange first reminded his readers about the way in which the roots t of the resolvent appear as a function of the roots $x', x'', \ldots x^{(m)}$ of the original equation and the powers of a primitive m^{th} root of unity α. His main goal in this excerpt was to deduce the degree of the resolvent equation, based on the total number of roots which can be formed in this way.

[20] The symmetric functions given by the coefficients of the polynomial $\prod_{k=1}^{m}(x - x_k)$ are called the ***elementary symmetric polynomials***. An example of a non-elementary symmetric function on three variables is given by $x_1^2 + x_2^2 + x_3^2$.

Let t be the unknown of the resolvent equation; in keeping with what was just said, we set

$$t = x' + \alpha x'' + \alpha^2 x''' + \alpha^3 x^{(iv)} + \ldots + \alpha^{m-1} x^{(m)},$$

the quantity α being one of the m^{th} roots of unity, that is to say, one of the roots of the binomial equation $y^m - 1 = 0$. . . . . .

It is first of all clear that, in the expression t, one can interchange the roots x', x'', x''', . . . , $x^{(m)}$ at will since there is nothing to distinguish them here from one and another; from this it follows that one obtains all the different values of t by making all possible permutations of the roots $x', x'', x''', \ldots, x^{(m)}$ and these values will necessarily be the roots of the resolvent in t which we wish to construct.

Now one knows, by the theory of combinations, that the number of permutations which can be obtained from m things is expressed in general by the product $1.2.3 \ldots m$; but we are going to see that this equation is capable of being reduced by the very form of its roots.

Task 12 Consider the case $m = 3$ and let x', x'', x''' denote the three roots of an arbitrary cubic equation and α denote a primitive cubic root of unity. According to Lagrange's analysis in the preceding excerpt, the resolvent for the given cubic will have a total of $3! = 6$ roots, arising from the $3! = 6$ possible permutations of x', x'', x''' in the given formula. Complete the list of these six roots below.

t	$=$	$x' + \alpha x'' + \alpha^2 x'''$		t	$=$		t	$=$
t	$=$	$x' + \alpha x''' + \alpha^2 x''$		t	$=$		t	$=$

The previous task illustrates how permuting the roots of the original equation in the formula for the resolvent's roots produces $m!$ resolvent roots in the specific case of $m = 3$. Of course, since $m! > m$ for $m > 2$, Lagrange's conclusion that an equation of degree m has a resolvent equation of degree $m!$ hardly seems like progress. But remember what we've seen in our example of the cubic equation $x^3 + nx + p = 0$: even though the original degree 3 equation has a resolvent equation of degree 6, that resolvent is quadratic in form, allowing us to use substitution to reduce the resolvent degree to just 2. Lagrange ended the preceding excerpt with the claim that a similar reduction in the degree of the resolvent is always possible, for any polynomial of any degree.[21] As Lagrange emphasized throughout his work, the key to this reduction will be to consider the *form* of these roots, $t = x' + \alpha x'' + \alpha^2 x''' + \ldots + \alpha^{m-1} x^{(m)}$, and the effect of permutations on this form. To set the stage for our reading of Lagrange's analysis of the general case, we return to the specific cubic equation example $x^3 + nx + p = 0$ and complete the proof that the roots of its resolvent equation do indeed assume this form.

[21] Once this reduction is achieved, the next question will be whether the reduced degree is sufficiently small that one could proceed to find an algebraic solution with known methods; if not, then some further reduction in the resolvent's degree would be required to complete the process.

A Specific Resolvent Example: Part III

In this example, we return to our exploration of the cubic equation $x^3 + nx + p = 0$, for which $n, p \in \mathbb{R}^+$ and its sixth degree resolvent equation is $t^6 + 27pt^3 - 27n^3 = 0$.

Denoting the real roots of the resolvent as t_1, t_2 and letting α be a primitive cubic root of unity, recall that the six roots of the resolvent are:

$$t_1 \qquad t_3 = \alpha t_1 \qquad t_5 = \alpha^2 t_1 \qquad ; \qquad t_2 \qquad t_4 = \alpha t_2 \qquad t_6 = \alpha^2 t_2,$$

Further recall that the three roots of the given cubic can be written as follows:

$$x' = \tfrac{1}{3}(t_1 + t_2) \qquad x'' = \tfrac{1}{3}(t_4 + t_5) \qquad x''' = \tfrac{1}{3}(t_3 + t_6)$$

Let's now look at how the six roots of the resolvent can be obtained via permutations of x', x'', x''' in the expression $t = x' + \alpha x'' + \alpha^2 x'''$.

(i) We first note the following useful fact[a] about sums of powers of primitive cubic roots of unity:

$$1 + \alpha + \alpha^2 = 0$$

(ii) Substituting the above values for x', x'', x''' and t_3, t_4, t_5, t_6 into the expression $x' + \alpha x'' + \alpha^2 x'''$, then simplifying using the facts that $\alpha^3 = 1$ and $1 + \alpha + \alpha^2 = 0$, we obtain:

$$\begin{aligned} x' + \alpha x'' + \alpha^2 x''' &= \tfrac{1}{3}(t_1 + t_2) + \alpha\left(\tfrac{1}{3}(t_4 + t_5)\right) + \alpha^2\left(\tfrac{1}{3}(t_3 + t_6)\right) \\ &= \tfrac{1}{3}\left[(t_1 + t_2) + \alpha\left(\alpha t_2 + \alpha^2 t_1\right) + \alpha^2\left(\alpha t_1 + \alpha^2 t_2\right)\right] \\ &= \tfrac{1}{3}\left(t_1 + \alpha^3 t_1 + \alpha^3 t_1\right) + \tfrac{1}{3}\left(t_2 + \alpha^2 t_2 + \alpha^4 t_2\right) \\ &= \tfrac{1}{3}t_1(3t_1) + \tfrac{1}{3}t_2 \underbrace{(1 + \alpha^2 + \alpha)}_{0} \;=\; t_1 \end{aligned}$$

A similar computation shows that $x' + \alpha x''' + \alpha^2 x'' = t_2$.

(iii) Using the fact that $\alpha(x' + \alpha x'' + \alpha^2 x''') = x''' + \alpha x' + \alpha^2 x''$, along with the result of part (ii), we obtain:

$$x''' + \alpha x' + \alpha^2 x'' = \alpha(x' + \alpha x'' + \alpha^2 x''') = \alpha t_1 = t_3$$

Then using the fact that $\alpha^2(x' + \alpha x''' + \alpha^2 x'') = x''' + \alpha x'' + \alpha^2 x'$ along with the result of part (ii) similarly allows us to conclude that $x''' + \alpha x'' + \alpha^2 x' = t_6$.

(iv) Similar computations can then be done *(do these!)* to determine which of the remaining two permutations of x', x'', x''' in the general formula $t = x' + \alpha x'' + \alpha^2 x'''$ correspond to the remaining two resolvent roots, t_4 and t_5.

---

[a] One way to verify this useful fact ($1 + \alpha + \alpha^2 = 0$) is by direct computation, remembering that since α is not specified to be any particular primitive cubic root of unity, there are technically two cases to check: $\alpha = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ and $\alpha = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$. (A geometric diagram is suggestive of what is happening in this sum, but does not constitute a proof!)

Alternatively, we can verify that $1 + \alpha + \alpha^2 = 0$ by factoring $\alpha^3 - 1 = (\alpha - 1)(\alpha^2 + \alpha + 1)$, and then applying the given assumptions $\alpha^3 = 1$, $\alpha \neq 1$ to conclude that the second factor must equal 0.

We now return to Lagrange's argument that, given any m^{th} degree polynomial, it is always possible to reduce the degree of the resolvent equation to a number less than $m!$. As you read through the first of these two excerpts, remember that Lagrange has already established that every permutation of $x', x'', x''', \ldots$ in the expression t will result in a root of the resolvent equation.

One first sees that this expression is an unvariable function of the quantities $\alpha^0 x'$, $\alpha x''$, $\alpha^2 x'''$, ..., and also that the result of permuting the roots x', x'', x''', ... among themselves will be the same as that of [permuting] the powers of α among themselves.

It follows from this that αt will be the result of the simultaneous permutations of [substituting] x' in for x'', x'' in for x''', $\ldots x^{(m)}$ in for x', since $\alpha^m = 1$. Similarly, $\alpha^2 t$ will be the result of the simultaneous permutations of [substituting] x' in for x''', x'' in for x^{iv}, $\ldots x^{(m-1)}$ in for x' and $x^{(m)}$ in for x'', since $\alpha^m = 1$, $\alpha^{m+1} = \alpha$, and so on.

Task 13 Consider the case $m = 3$, so that $t = x' + \alpha x'' + \alpha^2 x'''$ and $\alpha^3 = 1$.

(a) Write the expression which results from t under the permutation[22] of roots that simultaneously substitutes x' in for x'' , x'' in for x''' and x''' in for x'.

(b) Write the expression which results from t under the permutation of powers[23] of α that simultaneously substitutes α in for α^0 , α^2 in for α , and α^0 in for α^2.

(c) Compare the results of (a) and (b), and comment on how this illustrates that 'the result of permuting the roots $x', x'', x''', \ldots$ among themselves will be the same as that of [permuting] the powers of α among themselves.'

(d) Now determine the product αt and compare it to the results of parts (a) and (b). Explain why this proves that αt is also a root of the resolvent.

(e) Determine the permutation of the powers of α that corresponds to the permutation of roots that simultaneously substitutes x' in for x''', x'' in for x' and x''' in for x''. How could we obtain this same expression as a product of t by a power of α?

[22] One way to represent this permutation is with a function table such as the following, where the top row represents the inputs and the bottom row represents the output value to be substituted in place of each input:

$$\begin{pmatrix} x'' & x''' & x' \\ x' & x'' & x''' \end{pmatrix}$$

Although Lagrange himself did not use this particular representation, it was introduced soon afterwards by the French mathematician Cauchy.

[23] Representing this permutation with Cauchy's notation (described in the previous footnote) gives:

$$\begin{pmatrix} \alpha^0 & \alpha & \alpha^2 \\ \alpha & \alpha^2 & \alpha^0 \end{pmatrix}$$

We now continue with the remainder of Lagrange's argument that the degree of the resolvent can always be reduced to something less than $m!$.

> Thus, t being one of the roots of the resolvent equation in t, then αt, $\alpha^2 t$, $\alpha^3 t$, $\ldots \alpha^{m-1} t$ will also be roots of this same equation; consequently, the [resolvent] equation ... will be such that it does not change when t is replaced there by αt, by $\alpha^2 t$, by $\alpha^3 t$, ..., by $\alpha^{m-1} t$, from which it is easy to conclude first that this equation can only contain powers of t for which the exponent will be a multiple of m.
>
> If therefore one substitutes $\theta = t^m$, one will have an equation in θ which will be of degree only $1.2.3 \ldots [m-1]$.

Let us pause here to consider exactly what Lagrange has just claimed, and why he believed his claims to be true. Based on Task 13, the first claim in the excerpt should seem quite believable; namely,

> Thus, t being one of the roots of the resolvent equation in t, then αt, $\alpha^2 t$, $\alpha^3 t$, $\ldots \alpha^{m-1} t$ will also be roots of this same equation.

Note that no claim has been made that these m resolvent roots $(t\,,\, \alpha t\,,\, \alpha^2 t\,,\, \alpha^3 t, \ldots, \alpha^{m-1} t)$ are distinct, but only that this list accounts for m of the $m!$ roots of the resolvent. Lagrange continued by stating, without proof, the following consequence of this fact:

> ... consequently, the [resolvent] equation ... will be such that it does not change when t is replaced there by αt, by $\alpha^2 t$, by $\alpha^3 t$, ..., by $\alpha^{m-1} t$, **from which it is easy to conclude first that this equation can only contain powers of t for which the exponent will be a multiple of m.**

To get an idea of what Lagrange meant here, remember that his overall plan is to build up the resolvent equation 'by means of its roots' — in other words, by using what we would now call the Factor Theorem. Let's see how this plan plays out for the case of a general cubic equation.

A General Resolvent Equation Example

Start with an arbitrary cubic equation (so that $m = 3$), and denote its roots by x' , x'', and x'''.

Take α to be either primitive cubic root of unity.[a]

Let t_1, t_2 denote the following two roots of the resolvent equation:[b]

$$\begin{aligned} t_1 &= x' + \alpha x'' + \alpha^2 x''' \\ t_2 &= x' + \alpha x''' + \alpha^2 x'' \end{aligned}$$

We then know that the full set of all six roots of the resolvent is as follow:[c]

$$t_1\,,\ \alpha t_1\,,\ \alpha^2 t_1 \quad ; \quad t_2\,,\ \alpha t_2\,,\ \alpha^2 t_2.$$

By the Factor Theorem, we can thus write the resolvent equation in the form

$$(t - t_1)(t - \alpha t_1)(t - \alpha^2 t_1)(t - t_2)(t - \alpha t_2)(t - \alpha^2 t_2) = 0.$$

Notice that these six factors can be grouped to give two separate cubic functions:

$$g_1(t) = (t - t_1)(t - \alpha t_1)(t - \alpha^2 t_1) \qquad ; \qquad g_2(t) = (t - t_2)(t - \alpha t_2)(t - \alpha^2 t_2).$$

Expanding each separately, it is straightforward[d] to show that

$$g_1(t) = t^3 - t_1^3 \quad \text{and} \quad g_2(t) = t^3 - t_2^3.$$

Piecing these back together, the resolvent equation is thus given by the following function of t^3:

$$(t^3 - t_1^3)(t^3 - t_2^3) = 0,$$

for which the expanded form clearly contains only powers of t for which the exponent is a multiple of $m = 3$:

$$t^6 - (t_1^3 + t_2^3)t^3 + (t_1 t_2)^3 = 0.$$

---

[a] Although there are two primitive cubic roots of unity, $-\frac{1}{2} + \frac{\sqrt{3}}{2}i$ and $-\frac{1}{2} - \frac{\sqrt{3}}{2}i$, the argument outlined below does not depend on which of these is used.

[b] Note that we are *not* assuming that t_1 and t_2 are real-valued here! Nor are we assuming that $t_1 \neq t_2$. Rather, we are only assuming that t_1, t_2 are the roots of the sixth degree resolvent equation given by these particular arrangements of x', x'', x''' in the formula for the resolvent's roots. Our choice of which of the six possible arrangements to label as t_1 was completely arbitrary (other than a desire to maintain consistency with the notation used in the example of the specific cubic equation $x^3 + nx + p = 0$). Once t_1 was selected, however, our choice for t_2 had to differ from the arrangements given by t_1, αt_1 and $\alpha^2 t_1$ (for reasons which should become clear later in this task).

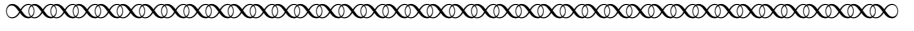
[c] In our analysis from Part I of the specific cubic equation example $x^3 + nx + p = 0$, we arrived at these same conclusions by substituting values into the resolvent equation which we already knew to be quadratic in form. We can not do that in this general case, since we are now trying to *prove* the resolvent is quadratic in form.

[d] To check this — and you should check this! — it may be useful to review Task 10 to recall how the elementary symmetric functions can be used to avoid literally multiplying out this expression.

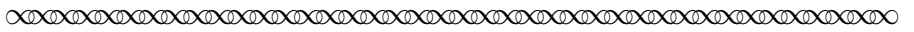
Notice that we can take this example one step further, since the final form of the resolvent allows us to make the substitution $\theta = t^3$, which reduces the resolvent equation to a quadratic:

$$(\theta - t_1^3)(\theta - t_1^3) = 0.$$

In other words, starting from a polynomial of degree $m = 3$, the resolvent equation of degree $m! = 6$ will always reduce (after a substitution) to an equation of degree $(m-1)! = 2! = 2$ — just as Lagrange claimed is the case in the final sentence of the last excerpt:



> If therefore one substitutes $\theta = t^m$, one will have an equation in θ which will be of degree only $1.2.3 \ldots [m-1]$.



In Task 14, you will examine this claim for the case of $m = 4$. Unfortunately, despite the fact that the resolvent 'can only contain powers of t for which the exponent will be a multiple of m' reduces the degree of the resolvent from $m!$ to $(m-1)!$, some difficulty remains even with relatively small values of m. Granted, a resolvent for a quintic equation undergoes a reduction from degree $5! = 120$ down to degree $4! = 24$ — but 24 is still *considerably* larger than the original equation's degree of 5.

Although a similar problem would seem to arise for quartics, where the initial resolvent degree of $4! = 24$ is reduced only to $3! = 6$, Lagrange used other arguments to show that the resolvent in this case ($m = 4$) could be further reduced to just a cubic equation.[24] He also explained how this reduction relates to the effect of permuting $x', x'', x''', x^{(iv)}$ in the expression for the resolvent's roots t, again focusing on the *form* of the expression in question. In essence, he showed that the resolvent root t can be written in a sufficiently symmetric way that only 3 'values' arise when $x', x'', x''', x^{(iv)}$ are permuted in all possible ways. More specifically, Lagrange showed that $t = \frac{x'x'' + x'''x^{(iv)}}{2}$, and that this (nearly symmetric) expression assumes only three distinct forms when $x', x'', x''', x^{(iv)}$ are permuted in all 24 possible ways — check this if you like!

Despite his success with polynomials of degree 3 and 4, Lagrange suspected (and Abel and Galois later confirmed) that it is not always possible to express the resolvent roots of equations in a form that is sufficiently symmetric to achieve a similar result for polynomials of degree five and higher. Nevertheless, Lagrange's introduction of permutations into the picture was the first significant step forward in centuries in the study of algebraic solvability. It also paved the way for Cauchy's development of a more general theory of permutations and a second important type of group called a *permutation group*. The similarities between the algebraic structure of the set of roots of unity and the algebraic structure of a permutation group in turn promoted further Cayley's ability to eventually define the notion of a completely abstract group that is now the object of study in every abstract algebra course. But that is the subject of the next phase of the evolution of the abstract group structure — with Task 14 on the following page, we bring the particular story of Lagrange's contributions to that evolution to a close.

[24] The strategy of reducing a quartic to a cubic was known to Renaissance algebraists; see footnote 3.

Task 14 This task outlines a rigorous proof of Lagrange's claim that the resolvent 'can only contain powers of t for which the exponent will be a multiple of m' in the case of $m = 4$.

Let x', x'', x''', $x^{(iv)}$ denote the four roots of an arbitrary quartic equation.

Let α be a primitive fourth root of unity.[25]

(a) Show that the 4!=24 roots of the resolvent for the given quartic can be partitioned into six disjoint sets of 4 roots, each of which has the form $S_i = \{t_i\,,\ \alpha t_i\,,\ \alpha^2 t_i\,,\ \alpha^3 t_i\,\}$, where $i \in \{1, 2, 3, 4, 5, 6\}$ and t_i is a particular root of the resolvent.

You might start, for example, by setting

$$t_1 \;=\; x' + \alpha x'' + \alpha^2 x''' + \alpha^3 x^{(iv)}\ .$$

To abbreviate writing, denote the order in which the four roots appear in this expression by '1, 2, 3, 4' and note that the set $S_1 = \{t_1\,,\ \alpha t_1\,,\ \alpha^2 t_1\,,\ \alpha^3 t_1\,\}$ contains the roots corresponding to the following formal expressions:

$$\begin{array}{rcll} t_1 & = & x' + \alpha x'' + \alpha^2 x''' + \alpha^3 x^{(iv)} & (1,2,3,4) \\ \alpha t_1 & = & x^{(iv)} + \alpha x' + \alpha^2 x'' + \alpha^3 x''' & (4,1,2,3) \\ \alpha^2 t_1 & = & x''' + \alpha x^{(iv)} + \alpha^2 x' + \alpha^3 x'' & (3,4,1,2) \\ \alpha^3 t_1 & = & x'' + \alpha x''' + \alpha^2 x^{(iv)} + \alpha^3 x' & (2,3,4,1) \end{array}$$

You can then choose t_2 to be any of the remaining 20 expressions obtained by some other permutation of $x', x'', x''', x^{(iv)}$ in the formula for the resolvent roots.

Explain how you can now be sure that the formal expressions for the elements in the set $S_1 = \{t_1\,,\ \alpha t_1\,,\ \alpha^2 t_1\,,\ \alpha^3 t_1\,\}$ are distinct from those in the set $S_2 = \{t_2\,,\ \alpha t_2\,,\ \alpha^2 t_2\,,\ \alpha^3 t_2\,\}$.

Then determine suitable values of t_3, t_4, t_5, t_6 (without necessarily writing out the full formal expression for each) and explain how you are sure the sets S_1, S_2, S_3, S_4, S_5, S_6 are mutually disjoint with respect to formal expressions.

(b) For $i \in \{1, 2, 3, 4, 5, 6\}$, let $g_i(t) = (t - t_i)(t - \alpha t_i)(t - \alpha^2 t_i)(t - \alpha^3 t_i)$.
Show that $g_i(t) = t^4 - t_i^4$.

Hint? To avoid literally multiplying out the four factors in g_i, it may be helpful to review Task 10 and instead write out the elementary symmetric functions that define the coefficients of a quartic $t^4 - At^3 + Bt^2 - Ct + D$ in terms of its roots. Also remember that α is a primitive fourth root of unity (either i or $-i$), and think about the values of $\alpha^2 + 1$ and $1 + \alpha + \alpha^2 + \alpha^3$ in either case.

(c) Conclude that the resolvent is a function of t^4, and explain why it can therefore be treated as a polynomial of degree 6 only. Why is this *not* a sufficient reduction to complete the algebraic solution of the original quartic?

[25] Although there are also two primitive fourth roots of unity, i and $-i$, the argument outlined below does not depend on which of these is used. Be careful not to implicitly assume that $\alpha = i$ in your proof!

APPENDIX I: Optional exercises on algebraic solvability of $x^5 - 1 = 0$

From our reading of Lagrange, we know that the five fifth roots of unity are given by the following trigonometric expressions:

$$x = \cos\left(\frac{2\pi k}{5}\right) + i\sin\left(\frac{2\pi k}{5}\right), \text{ for } k = 1, 2, 3, 4, 5$$

Note that it is not be immediately obvious that these (trigonometric) values can be expressed in the proper (algebraic) form. Indeed, Lagrange commented (page 9 of project) that the general problem of proving this for roots of unity is one that "mathematicians have greatly occupied themselves with ..." , and commended Gauss' eventual (1801) proof of this fact for being "as original as it was ingenious." For the specific case of the fifth roots of unity, however, Lagrange also noted (in footnote 14) that these can be (algebraically) expressed as follow:

$$1 \ , \ \frac{\sqrt{5}-1}{4} \pm \frac{\sqrt{10+2\sqrt{5}}}{4}i \ , \ -\frac{\sqrt{5}+1}{4} \pm \frac{\sqrt{10-2\sqrt{5}}}{4}i$$

Task I

Verify that Lagrange's values are correct by (algebraically) solving the equation $x^5 - 1 = 0$ as follows.

- Begin by factoring the equation $x^5 - 1 = 0$ to obtain: $(x-1)(x^4+x^3+x^2+x+1) = 0$

  The first factor gives the obvious fifth root, $x = 1$.

  Thus, we need only (algebraically) solve the equation associated with the second factor: $x^4 + x^3 + x^2 + x + 1 = 0$
- Divide this (fourth-degree) equation by x^2 to obtain: $x^2 + x + 1 + \frac{1}{x} + \frac{1}{x^2} = 0$

  (How do we know that it is okay to do this?)
- Now use the (clever) substitution $y = x + \frac{1}{x}$ to obtain a quadratic equation in y. Use the quadratic formula to (algebraically) solve this equation.
- After (algebraically) solving the quadratic equation from the previous step for y, 'undo' the substitution $y = x + \frac{1}{x}$ to obtain the (four) complex-valued solutions of $x^5 - 1 = 0$ which were stated by Lagrange. *(The quadratic formula will be needed again here.)*

Task II

Use Lagrange's values for the fifth roots of unity to algebraically express (e.g., using only elementary arithmetic operations and extraction of roots) the following trigonometric values, and explain how you know these are correct:

$$\cos\left(\tfrac{2\pi}{5}\right) \qquad \cos\left(\tfrac{4\pi}{5}\right) \qquad \cos\left(\tfrac{6\pi}{5}\right) \qquad \cos\left(\tfrac{8\pi}{5}\right)$$

$$\sin\left(\tfrac{2\pi}{5}\right) \qquad \sin\left(\tfrac{4\pi}{5}\right) \qquad \sin\left(\tfrac{6\pi}{5}\right) \qquad \sin\left(\tfrac{8\pi}{5}\right)$$

APPENDIX II: Optional exercises on de Moivre's and Euler's Formulas

The following tasks explore proofs of the following famous formulas, discussed in Subsection 1.1:

$$\textbf{de Moivre's Formula:} \quad (\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$$
$$\textbf{Euler's formula:} \quad e^{i\theta} = \cos\theta + i\sin\theta$$

Task I

Let $x = \cos\left(\frac{2\pi k}{m}\right) + i\sin\left(\frac{2\pi k}{m}\right)$ where $k \in \{1, 2, 3, \ldots, m\}$.
Use de Moivre's formula to show that $x^m = 1$.

Task II

This exercise outlines a proof of de Moivre's formula for natural numbers n, based only on trigonometric sum identities and induction.

Recall the following trigonometric identities:

$$\cos(x+y) = \cos x\cos y - \sin x\sin y \quad ; \quad \sin(x+y) = \cos x\sin y + \cos y\sin x$$

(a) Prove that de Moivre's formula holds for $n = 2$ by expanding $(\cos\theta + i\sin\theta)^2$ and applying the sum identities with $x = y = \theta$.

(b) Use the result of part (a) to expand $(\cos\theta + i\sin\theta)^3$; then use the sum identities with $x = \theta$ and $y = 2\theta$ to prove de Moivre's formula holds for $n = 3$.

(c) Use the sum identities and induction on n to prove de Moivre's formula in the case where n is a natural number.

Task III

Use the power series for e^x, $\sin x$ and $\cos x$ given below to prove Euler's formula.[26]
Recall that $i^2 = -1$, $i^3 = -i$ and $i^4 = 1$.

$$e^x = \sum_{k=0}^{\infty} \frac{1}{k!}x^k \qquad \sin x = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)!}x^{2k+1} \qquad \cos x = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k)!}x^{2k}$$

Note: Recall that all three series are absolutely convergent on $\mathbb{R}$; thus, we can legitimately rearrange their terms, without in so doing changing the values to which they converge.

[26] Euler's derivation of this formula used a somewhat different approach in which infinitesimals appeared.

References

Raymond Clare Archibald. *Benjamin Peirce, 1809–1880: Biographical Sketch and Bibliography.* The Mathematical Association of America, Oberlin, OH, 1925.

Arthur Cayley. On the theory of groups, as depending on the symbolic equation $\theta^n = 1$ - Part I. *Philosophical Magazine*, 7:151–242, 1854. Also in *The Collected Mathematical Papers of Arthur Cayley*, Cambridge: Cambridge University Press, Volume 2 (1889), 123–130.

J. L. Lagrange. Réflexions sur la résolution algébrique des équations. *Mémoire de l'Académie de Berlin*, 1770-1771. Also in *Œuvres complètes de Lagrange*, Tome 3, 205-421.

J. L. Lagrange. *Traité de la résolution des èquations numériques de tous les degrés, avec des notes sur plusieurs points de la théorie des équations algébriques.* Courcier, Paris, 1808.

Hans Wussing. *The Genesis of the Abstract Group Concept: A Contribution to the History of the Origins of Abstract Group Theory.* MIT Press, Cambridge and London, 1984.

Notes to Instructors

This Primary Source Project (PSP) draws on works by one of the early precursors of abstract group, French mathematician J. L. Lagrange (1736-1813). An important figure in the development of group theory, Lagrange made the first real advance in the problem of solving polynomial equations by radicals since the work of Cardano and his sixteenth century contemporaries. In particular, Lagrange was the first to suggest the existence of a relation between permutations and the solution of equations by radicals, a suggestion later exploited by Abel and Galois. In addition to the important group-theoretic concept of a permutation, the project employs excerpts from Lagrange's study of roots of unity to develop the concept of a finite cyclic group. Lagrange's description of his quest for a general method of algebraically solving all polynomial equations is also a model of mathematical research that make him a master well worth reading by today's students of mathematics. Through their guided reading of excerpts from Lagrange, students thus encounter his original motivations while developing their own understanding of these important group-theoretic concepts via the very familiar and concrete context of solving polynomial equations.

Absolutely no familiarity with group theory is assumed in this PSP! Instead, it was explicitly designed to serve as students' very first encounter with group-related ideas. This approach has been tested with good effect by instructors at a variety of institutions who have taught with its parent PSP, an extended primary source project entitled *Abstract Awakenings in Group Theory* that was developed with funding from a prior NSF grant.[27]

In fact, the current PSP is based on the first section of that earlier PSP, which then goes on to develop a significant portion of the core topics in elementary group theory from the standard curriculum of a one semester junior-level abstract algebra course.[28] Instructors who begin their study of group theory with the PSP *The Roots of Early Group Theory in the Works of Lagrange* and then wish to continue with the pedagogy of primary source projects throughout their students' study of group theory could thus easily shift over to the PSP *Abstract Awakenings of Algebra*.[29]

---

[27]The full title of this earlier PSP (developed under the NSF grant DUE-0715392) is *Abstract Awakenings in Group Theory: Early group theory in the works of Lagrange, Cauchy, and Cayley.* Its centerpiece is the 1854 inaugural paper on abstract group, Arthur Cayley's *On the theory of groups, as depending on the symbolic equation* $\theta^n = 1$ [Cayley, 1854]. In keeping with the historical record, and to provide concrete examples on which to base their abstraction of the group concept, Section 1 of that project begins with the material from Lagrange in the PSP that you are currently reading. Section 2 then employs selections from writings by Augustin Cauchy in which a more general theory of permutations and symmetric groups was developed independently of the theory of equations, and today's current notation for permutations was first introduced. Section 2 also includes Cauchy's statement and proof of Lagrange's Theorem for Symmetric Groups, both of which are easily adapted to the more general case of any finite group. The project then turns to a detailed reading of Cayley's complete paper in Sections 3 and 4, paying careful attention to the similarities between the theory of permutation groups as it was developed by Cauchy and the modern notion of an abstract group as it was unveiled by Cayley.

[28]Topics developed in the PSP *Abstract Awakenings in Group Theory* include roots of unity, permutations, definition and elementary properties of group (including results related to the order of group elements), abelian groups, cyclic groups, symmetric groups, alternating groups, Cayley tables, Lagrange's Theorem, group isomorphisms, classification of groups of small order, and direct products. The concept of cosets are also introduced in the main body of the project, and further developed in an appendix which also states the definitions of normal subgroup and factor group. Completion of the entire project takes approximately 10 weeks, but (un)covers the vast majority of the elementary group theory typically studied in a junior level abstract algebra course.

[29]To obtain the most recent version of *Abstract Awakenings in Group Theory*, contact the author at

For those who prefer a less extended use of this instructional practice, the PSP *The Roots of Early Group Theory in the Works of Lagrange* could also be used in conjunction with a more traditional textbook. In either case, this PSP will be more effective as an exploratory introduction to the group concept if it is used *before* students have studied the concepts of cyclic groups and permutations / permutations groups in much, if any, detail.

Classroom implementation of this and other PSPs may be accomplished through individually assigned work, small group work and/or whole class discussion. A combination of these instructional strategies is recommended in order to take advantage of the variety of questions included in the project. To reap the full pedagogical and mathematical benefits offered by the PSP approach, students should be required to read assigned sections and complete advance work on tasks related to that reading prior to in-class discussions. The author's method of ensuring that advance reading takes place is to require student completion of "Reading Guides" (or "Entrance Tickets"); see pages 36–37 below for a sample guide based on this particular PSP.[30] The author's students do receive credit for completion of each Reading Guide, but with no penalty for errors in solutions.

A sample implementation schedule is recommended on pages 34–35 below. The following description of the content of each section of the PSP should assist instructors in determining how best to adapt that recommended schedule to their own course goals and students' needs.

- Section 1: Introduction
  This section includes a broad overview of the early history of the theory of equations, as it relates to the eventual development of group theory. This material is intended to provide students with a context for their study of Lagrange's work in this PSP, and for their later study of the more abstract concept of a group.
- Section 2: Lagrange on the algebraic solution of equations
  The primary objective of this section is to introduce the language and notation used by Lagrange in his analysis of the problem of solving equations by radical. The concept of a 'resolvent equation' is discussed in the context of Lagrange's motivation for studying such equations. A very concrete example, based on a problem initially solved by Cardano, is given to illustrate how a resolvent equation can be used to solve a polynomial equation. Aspects of this example are also considered in later parts of the project, in connection with Lagrange's work on roots of unity and permutations. Examining this example in this way[31] connects well with students' prior, largely procedural, experiences with algebra, thereby providing a nice bridge between their former and future algebraic studies.

`janet.barnett@csupueblo.edu`, or visit `www.cs.nmsu.edu/historical-projects/projects.php` for an earlier version. Within that earlier version, all resolvent equation examples are instead presented as tasks for students to complete themselves. An alternative version of the PSP *The Roots of Early Group Theory in the Works of Lagrange* which adopts that more open-ended/inquiry-based approach is also available upon request from the author.

[30]The author's Reading Guides typically include "Classroom Preparation" exercises (drawn from the PSP Tasks) for students to complete prior to arriving in class; they may also include "Discussion Questions" that ask students only to read a given task and jot down some notes in preparation for class work. On occasion, tasks are also assigned as follow-up to a prior class discussion. In addition to supporting students' advance preparation efforts, these guides provide helpful feedback to the instructor about individual and whole class understanding of the material.

[31]The author's decision to present this and other resolvent equations in the PSP as examples (rather than tasks for students to work through themselves) is due to the fact that resolvent equations themselves are no longer a focal point in the study of group theory. As noted in a previous footnote, however, an alternate version of the PSP which presents these examples as student tasks is available upon request.

- Section 3: Roots of unity in Lagrange's analysis
  This section introduces students to the concept of finite cyclic groups via the context of Lagrange's writing on the solution of equations. Current notation and terminology for cyclic groups is included. Two particular tasks in this section are especially critical. Task 8 leads students through a particular proof of Lagrange's claim that every non-unity complex m^{th} root of unity β is a generator of the (cyclic) group formed by the m^{th} roots of unity in the case where m is a prime. The proof strategy in question takes advantage of the fact that U_m is finite by having students prove that $< \beta > \subseteq U_m$ with $| < \beta > | = m$, in order to conclude that $< \beta > = U_m$. Task 9 then asks students to explore and prove a conjecture about which complex m^{th} root of unity is a generator of the (cyclic) group formed by the m^{th} roots of unity in the case where m is a composite. Both these exercises allow students to draw on the very concrete context of complex numbers, but without assuming much in terms of background knowledge about the complex numbers. The proofs generated by students within this familiar context also provide a good basis for proving these same results in the more general case of an arbitrary cyclic group. The scaffolding offered by the proof outline given in Task 8 is intended to offer students further support in their early efforts at formal proof writing in abstract algebra.

- Section 4: Permutations of roots in Lagrange's analysis
  This section returns to Lagrange's analysis of the degree of the resolvent equation, in which the concept of a permutation naturally arises within the context of his writing on the solution of equations. The elementary symmetric functions are introduced as formulas that give the coefficients of a polynomial in terms of its roots; students find this a surprising and fascinating method of expanding the factored form of polynomial. The focus of the excerpts and tasks in this section, however, is on the concept of a permutations. The culminating resolvent equation example and the related Task 14 also offer a natural context for the concept of a n-cycle. Although operations on permutations are not introduced in this section, the modern notation for permutations and for n-cycles (both originally due to Cauchy) is introduced.

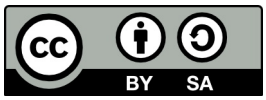
- Appendix I: Optional exercises on fifth roots of unity
  This optional appendix includes very straightforward exercises (involving little more than the quadratic formula) that are related to Lagrange's discussion of the algebraic solvability of equations of the form $x^m - 1 = 0$. Together with those in Appendix II, these exercises can be used to offer students an opportunity to begin practicing more formal mathematical writing, but within the familiar context of algebraic equations / manipulations (rather than proofs).

- Appendix II: Optional exercises on de Moivre's and Euler's Formulas
  This optional appendix includes exercises related to the material on roots of unity from Section 2, including a proof by induction of deMoivre's Theorem.

LaTeXcode of the entire PSP is available from the author by request to facilitate preparation of reading guides or 'in-class task sheets' based on tasks included in the project. The PSP itself can also be modified by instructors as desired to better suit their goals for the course.

Acknowledgments

The development of this student project has been partially supported by the Learning Discrete Mathematics and Computer Science via Primary Historical Sources project with funding from the National Science Foundation's Course, Curriculum & Laboratory Improvement Program (CCLI) Program under grant number 0715392, and by the Transforming Instruction in Undergraduate Mathematics via Primary Historical Sources (TRIUMPHS) project with funding from the National Science Foundation's Improving Undergraduate STEM Education (IUSE) Program under grant number 1523494. Any opinions, findings, and conclusions or recommendations expressed in this project are those of the author and do not necessarily reflect the views of the National Science Foundation.



For more information about Learning Discrete Mathematics and Computer Science via Primary Historical Sources, visit `https://www.cs.nmsu.edu/historical-projects/`.

For more information about Transforming Instruction in Undergraduate Mathematics via Primary Historical Sources (TRIUMPHS), visit `http://webpages.ursinus.edu/nscoville/TRIUMPHS.html`.

Sample PSP Implementation (based on a 55 minute class period)

- **Advance Preparation Work for Day 1** (to be completed before class)
  Read pages 1–9 in Sections 1 and 2, completing Tasks 1–2 for class discussion along the way, per the sample Reading Guide on pages 36–37 below.
- **Day 1 of Class Work**
  - Whole class and/or small group discussion of the following:
    * (Optional) Historical and mathematical ideas from Section 1 (Introduction), if desired
    * Mathematical concepts in Section 2, including answers to Task 1.
    * Resolvent Equation Example - Part I (page 7).
    * Assigned reading in Section 3, including answers to Task 2; this discussion could also be postponed for Day 2 of Class Work, after instructor's review students' advance work..
  - Time permitting, the instructor could preview the formulas on page 10, or have students continue reading (individually or in small group) Section 3, pages 10 – 11 (through Task 2).
  - **Homework (optional)**: A complete formal write-up of some or all of the Tasks in Appendices I and II could be assigned, to be due at a later date (e.g., one week after completion of the in-class work).

- **Advance Preparation Work for Day 2**
  In Section 3, read pages 10–14, completing Tasks 3, 4, 5, and 6(a) for class discussion along the way. (Depending on the general background of the students, the advance reading for Day 2 could also include page 15 and preparation of Task 7(a), but this is ambitious.)
- **Day 2 of Class Work**
  - Brief whole class discussion of terminology and notation introduced in advanced reading:
    de Moivre's Formula, *Euler's Formula*, *primitive root of unity*, etc.
    This could include review of the answers to some or all of the following: Tasks 3, 4, 5, 6(a).
  - Small group work on remaining parts of Task 6.
  - Time permitting, the instructor could preview the notation and terminology discussed on page 15, or have students continue reading (individually or in small group) Section 3, page 15 (through Task 7).

- **Advance Preparation Work for Day 3** (to be completed before class)
  Read page 15 and complete Task 7; also read through all parts of Task 8 (page 16), and prepare notes for class discussion.
- **Day 3 of Class Work**
  - Brief whole class discussion of terminology and notation introduced in advanced reading:
    U_m, $\langle\beta\rangle$, *primitive root of unity*, *generator*, etc.
    This could include answers to Task 7 by way of illustration.
  - Begin small group work on Task 8.
  - **Homework**: A complete formal write-up of student work on Task 8 a should be assigned, to be due at a later date (e.g., one week after completion of the in-class work).

- **Advance Preparation Work for Day 4** (to be completed before class)
  Review Task 8 in-class work from Day 3, and prepare notes for its continuation. Complete Task 9, part (a), and perhaps also the first portion of part (b).

- **Day 4 of Class Work**
  - Small group discussion of Task 8 and Task 9.
  - Summarizing whole class discussion of cyclic group ideas introduced in Section 3.
  - Time permitting, whole class or small group review and discussion of Resolvent Equation Example - Part II.

    Note: *Tasks 8 and 9(b) are the core material of Section 3. Depending on the student group, however, one day of in-class work may suffice for small group discussion of these two tasks. In this case, the Advance Preparation and In-class work listed above for Day 4 could instead be combined with that listed below for Day 5.*

- **Advance Preparation Work for Day 5** (to be completed before class)
  Finish reading Section 3 (last half of page 17). In Section 4, read pages 18–20, completing work on the following for class discussion along the way: some/all of Task 10, some/all of Task 11, and all of Task 12.

- **Day 5 of Class Work**
  - As desired for a segue to Section 4, whole class or small group review and discussion of Resolvent Equation Example - Part II.
  - Whole and/or small group discussion of the ideas in advance reading, to include answers to some/all of Tasks 10–12.
  - Time permitting, the instructor could preview the ideas discussed at the bottom of page 20.

- **Advance Preparation Work for Day 6** (to be completed before class)
  Complete reading of Section 4, pages 20–24.

- **Day 6 of Class Work**
  - Whole group discussion of ideas from assigned reading, including the General Resolvent Equation Example on page 24, completing work on some/all of Task 13 for class discussion along the way.
  - Summarizing whole group discussion of ideas related to permutations from Section 4.
  - Time permitting, begin small group work on Task 14.

- **Advance Preparation Work for (optional) Day 7** (to be completed before class)
  Read through Task 14, page 26, to prepare for small group work.

- **(Optional) Day 7 of Class Work**
  - Summarizing whole group discussion of ideas related to permutations from Section 4.
  - Small group work on Task 14.
  - **Homework** : A complete formal write-up of student work on Task 14 should also be assigned, to be due at a later date (e.g., one week after completion of the in-class work).

SAMPLE READING GUIDE

Background Information: The primary goal of this two-page reading and tasks assigned in this guide is tto familiarize students with Lagrange's notation and terminology related to resolvent equations in order to prepare them for in-class small group work on Task 1 and Task 2 .

****

Reading Assignment - *The Roots of Early Group Theory in the Works of Lagrange* - pp. 1 – 9.

1. Read the Introduction, pp. 1 – 4. *Jot down any comments or questions you have here.*

2. From Section 2, read pp. 4 – 5.

   Them **complete Task 1** (page 5) in preparation for class discussion here:

   Task 1 This task reviews some basic vocabulary and mathematical developments discussed in the introduction and the preceding Lagrange excerpt.

   (a) What do we mean when we say a polynomial equation is 'algebraically solvable'? For what degree polynomials were algebraic solutions known when Lagrange was writing?

   (b) What is a 'resolvent equation'? How does the degree of the resolvent equation compare to the degree of the given equation?

3. Now complete your reading of Section 2, by finishing pages 6–8.

   - What specific equation is being solved in the Example on page 7?

   - **Write at least one comment and at least one question about the ideas presented in this project thus far.**

4. In Section 3, read pages 8–9. *Jot down any comments or questions you have here.*

5. **DISCUSSION** Jot down your notes about Task 2 from page 10 here.

   Task 2 Without employing a calculator or computer, use the formula $x = \cos\left(\frac{2\pi k}{m}\right) + i \sin\left(\frac{2\pi k}{m}\right)$ (with $m = 6$) to express all sixth roots of unity in terms of the elementary arithmetic operations on rational numbers and their roots only.

   What difficulties do we encounter when you try to do this for the **fifth** roots of unity? (See footnote 14 on page 10 for Lagrange's list of the five fifth roots of unity.)