An Independent Theory of Permutations: Early Group Theory in the Work of A.-L. Cauchy

Janet Heine Barnett*

July 1, 2025

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 coefficients, 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 by the discovery that there is *no* algebraic formula for the roots of equations of degree 5 or higher, 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 with the discovery of this impossibility as the study of *structures* such as groups coming to occupy center stage.

The goal of this project is to look at one specific type of group — today, called the *symmetric group* — through selected excerpts from the writing of a mathematician involved in the early phases of its evolution: Augustin-Louis Cauchy (1789–1857). As we will see from Cauchy's own introduction to his work, that work grew out of efforts to find formulas for higher degree polynomial equations that linked relations between a type of function called a 'permutation' to the solution of equations by radicals. Beyond his historical comments in that introduction, however, there is little trace of those origins in Cauchy's work.[1] Rather, Cauchy's research is remarkable for the way in which it established a more general theory of permutations that was fully independent of the theory of equations.

In Section 1 of this project, we will study the basics of permutation theory through selections from Cauchy's writing. In Section 2, we then look at some more advanced features of that theory, including the proof of an important theorem in group theory that is commonly referred to as Lagrange's Theorem.

*Department of Mathematics and Physics; Colorado State University Pueblo; janet.barnett@csupueblo.edu.

[1] For more on this evolution as revealed through selections from the writings of the eighteenth-century French mathematician J. L. Lagrange (1736–1813), see the student project [Barnett, 2017].

In the concluding section, we comment briefly on later developments in the history of group theory and consolidate our understanding of Cauchy's contribution to that field using its modern notation.

1 Cauchy's Permutation Basics

Augustin-Louis Cauchy was born in Paris on August 21, 1789, the year the French Revolution began. His family moved to Arcueil, a town just outside of Paris, to avoid the turmoil of the revolution, and Cauchy spent his earliest days there. He was educated by his father, who counted a number of important scientists and mathematicians, including J. L. Lagrange (1736–1813), for whom Lagrange's Theorem is named, among his friends. It was Lagrange, in fact, who advised Cauchy's father that his son should obtain a good grounding in languages before starting a serious study of mathematics. Cauchy studied classical languages for two years before being trained as an engineer. He worked as an engineer in Cherbourg, France from 1810–1812, during which time he undertook his first mathematical researches. He then lived and worked as a mathematician in Paris for most of his remaining life, with the exception of eight years (1830–1838) of self-imposed exile from France for political reasons.[2] Even after returning to Paris in 1838, he refused to take an oath of allegiance to the political regime then in power and was unable to regain his various teaching positions. Cauchy's staunch royalism and his equally staunch religious zeal made him contentious, and his relations with other mathematicians and scientists were often strained.[3] Nevertheless, his mathematical contributions were (and still are) widely admired for their depth, their breadth, and their rigor. He is especially remembered for his efforts to reformulate the foundations of calculus in terms of limits defined via absolute value inequalities. Cauchy died near Paris in the village of Sceaux on May 23, 1857 after contracting a fever on a trip to the country to help restore his health, which had always been weak.

Cauchy's research on permutations was completed in two different periods, the first of which occurred around 1812. In that year, he presented a paper entitled *Essai sur les fonctions symétriques* to the French Academy of Sciences, the contents of which were later published in two articles in 1815.[4] He did not publish anything further on permutations until 1844–1846, when his extensive *Mémoire sur les arrangements que l'on peut former avec des lettres données* appeared, in addition to 27 shorter articles. In these later works, Cauchy made no mention of polynomial equations, focusing instead on the systematic development of the algebraic properties of permutations as interesting objects of study in their own right. In doing so, Cauchy established the theory of permutations as an independent branch of mathematics which could, by virtue of its generality, then be applied to a variety of mathematical problems; both Cauchy and British mathematician Arthur Cayley (1821–1895) made use of permutations in their work on the theory of determinants, for example.[5]

In the introduction of his earliest manuscript [Cauchy, 1815a], however, Cauchy made it clear that his

[2] Interestingly, Cauchy taught for a time in Turin, Italy, where Lagrange had his start, during this period of self-exile.

[3] Cauchy is particularly noted for being unsupportive of young mathematicians. For example, Niels Abel (1802–1829) and Évariste (1811–1832) Galois — both of whom are remembered today for their important contributions to the development of today's group theory — are known to have submitted papers to the French Academy of Sciences that were assigned to Cauchy for review; in each case, Cauchy either failed to return the papers promptly or lost them completely.

[4] See [Cauchy, 1815a,b] in the bibliography for their titles.

[5] To learn about Cauchy's work on determinants and how permutations entered into that work, see the student project Determining the Determinant", [Otero, 2018]. As we will see in the conclusion of this project, Arthur Cayley was also an important player in the historical development of today's group theory, in addition to his important work with determinants.

ideas about permutations were initially stimulated by the specific problem of algebraic solvability, and Lagrange's work in that area in particular. As you read the following excerpt from that introduction, it may be helpful to know that Lagrange had identified the number of distinguishable forms that result from the permuting the variables in an expression as a potential tool in studying algebraic solvability. It is this idea that Cauchy extended beyond the realm of formulas for the roots of a resolvent equation, applying it more generally to any function of n variables.

Memoire on the number of forms that a function can assume by permuting the quantities involved in all possible ways

Messieurs Lagrange and Vandermonde[6] were, I believe, the first to have considered functions of several variables relative to the number of forms they can assume when one substitutes these variables in place of each other. ... Since then, several Italian mathematicians have productively occupied themselves with this matter, and particularly Monsieur Ruffini.[7] ... One of the most remarkable consequences of the work of these various mathematicians is that, for a given number of letters, it is not always possible to form a function which has a specified number of forms.

Let's relate the final statement of this excerpt back to the work of Lagrange. We start with a positive result: namely, that it is possible to find a function $t(x_1, x_2, x_3, x_4)$ of 4 variables which has exactly 3 forms when its variables are permuted in all possible 4!=24 ways. In the context of Lagrange's analysis, the function t gave the roots of a resolvent equation[8] in terms of the roots x_1, x_2, x_3, x_4 of the original quartic polynomial, and the fact that t has just three distinct forms under permutations of these roots meant that the resolvent equation is a cubic (i.e., solvable by formula with just three roots).[9] On the other hand, the degree of the resolvent equation for a quintic can not in general be reduced to degree four, since it is impossible to construct a function of 5 variables $t(x_1, x_2, x_3, x_4, x_5)$ which has exactly 4 forms when the variables are permuted in all 5!=120 possible ways. As a natural follow-up to this and similar impossibility statements, Cauchy pursued the following question in his earliest manuscript on permutations: for a given number n of variables, what can be said about the possible number of distinct forms that a function of n variables *can* produce under permutations of those variables?

In developing an answer to this question, Cauchy introduced new notation for permutations which was far superior to that used by Lagrange. Our next excerpt, taken from Cauchy's 1844 manuscript on the theory of permutations [Cauchy, 1844], explains this notation.

[6] Alexandre-Théophile Vandermonde (1735–1796) was a French musician and musical theorist who wrote four mathematical papers between 1771 and 1773. The first of these considered the solvability of algebraic equations, and appeared nearly simultaneously with Lagrange's work on this same problem. Lagrange concluded his own 1808 note on algebraic solvability with a summary of 'the beautiful work done by Vandermonde.'

[7] The Italian mathematician Paolo Ruffini (1765–1822) published a proof that the quintic (5th degree) equation can not be solved algebraically in 1799, but his proposed proof contained a gap. Abel, who was not aware of Ruffini's work until 1826 when he (Abel) developed his own proof of that impossibility result, described Ruffini's proof as "so complicated that it is very difficult to decide the correctness of his reasoning" (as quoted in [Wussing, 1984, p. 97]).

[8] A resolvent equation is an equation associated with a given polynomial which has roots that are explicitly related to the roots of that given polynomial. In short, if one is able to solve the resolvent equation, then one can find the solution of the given polynomial equation, and vice versa.

[9] See the project [Barnett, 2017] for further detail.

Memoire on the arrangements that can be formed with given letters,
and on the permutations or substitutions which provide the passage from one arrangement to another

§1st - *General Considerations*

Let $x, y, z, \ldots$ be distinct letters, which we assume to represent independent variables. If we number the places occupied by these variables in a certain function Ω, and then write these variables $x, y, z \ldots$ in the order assigned to the places that they occupy, we obtain a certain *arrangement*

$$xyz \ldots,$$

and when the variables are displaced, this arrangement will be replaced by another, which can be compared to the first by knowing the nature of the displacements.

. . .

We call *permutation* or *substitution* the operation which consists of displacing these variables, by substituting them for each other, in the form given by the function Ω, or in the corresponding arrangement. To denote this permutation, we write the new arrangement that is produced *below* the original, and we close the system of these two arrangements between parentheses. Thus, for example, being given the function

$$\Omega = x + 2y + 3z,$$

where the variables x, y, z occupy respectively the first, the second and the third place, and consequently succeed each other in the order indicated by the arrangement

$$xyz,$$

if we exchange the variables y, z which occupy the two final places, we obtain a new form Ω' from Ω, which will be distinct from the first, and is determined by the formula

$$\Omega' = x + 2z + 3y.$$

Moreover, the new arrangement, corresponding to the new form, will be

$$xzy,$$

and the permutation by which we pass from the first form to the second will be represented by the notation[10]

$$\begin{pmatrix} xyz \\ xzy \end{pmatrix}$$

which indicates sufficiently the manner in which the variables have been displaced.

This done, the different forms of a function of n letters correspond evidently to the distinct arrangements that one can form with these n letters. Moreover, the number of these arrangements is, as we know, given by the product

$$1.2.3 \ldots n.$$

[10]Cauchy himself wrote the new arrangement *above* the original arrangement; throughout this project, we modify Cauchy's notation slightly so that it will be identical to that used in current texts.

We . . . put, as an abbreviation,

$$N = 1.2.3 \ldots n$$

. . .

Observe that we can, with no inconvenience, erase any letter that appears in the same place in the two terms of a given permutation, thereby indicating that the letter will not be displaced. Thus, in particular, we will have

$$\begin{pmatrix} xyz \\ xzy \end{pmatrix} = \begin{pmatrix} yz \\ zy \end{pmatrix},$$

which sufficiently indicates the manner in which the variables are displaced. The two arrangements xyz, xzy, included in this permutations, form that which we will call its *two terms*, or its *numerator* and its *denominator*.

Task 1 Let $\Omega = x + 2y + 3z$.

(a) Use Cauchy's notation to write the permutation associated with $\Omega'' = y + 2z + 3x$.

(b) Write the form Ω''' obtained from applying the permutation $\begin{pmatrix} xyz \\ zyx \end{pmatrix}$ to Ω .

Note that Cauchy used the term 'arrangement' when referring to an ordered list of variables (e.g., 'xyz', 'xzy'). Today, the term 'permutation' is often used for this purpose; this is especially common usage in probability and combinatorics, where the ordered list 'xzy' is called a permutation of the letters x, y, z. In group theory, the word 'permutation' continues to be used in Cauchy's sense of the word, and refers to the process which changes one arrangement (such as 'xyz') to another arrangement (such as 'xzy'). In other words, a ***permutation*** is a *function* which maps one set of objects (in this case, the letters x, y, z) onto the same set in a one-to-one fashion. The notation Cauchy used for permutations is especially well-suited to remind us of this, given its resemblance to a table of function values. Thus, if we let $f = \begin{pmatrix} xyz \\ xzy \end{pmatrix}$, then we would have $f(x) = x$, $f(y) = z$ and $f(z) = y$.

Cauchy himself used the terms 'permutation' and 'substitution' interchangeably in his later work. In the remainder of this project, we will use the term 'permutation' in our translation of his work into English, in keeping with current usage. In Section 1, we examine excerpts from his 1845 work which explain the notion of permutation multiplication and its basic properties. With these properties in hand, we then turn in Section 2 to Cauchy's study of the algebraic structure obtained by considering a set of permutations together with the operation of permutation multiplication, a structure known today as a *permutation group*.

1.1 Multiplying Permutations

Although he did not explicitly discuss the fact that permutations are one-to-one functions from a set onto itself,[11] Cauchy was certainly aware of their function nature. This is clear from the following excerpt, in

[11] A one-to-one onto function is also called a bijection.

which two types of products involving permutations are discussed. As you read this excerpt, notice that the first type of product — that of an arrangement by a permutation — simply treats the arrangement xyz as an input value for the function f defined by the permutation $\begin{pmatrix} xyz \\ xzy \end{pmatrix}$, with the function values $f(x), f(y), f(z)$ evaluated all at once. The second type of product — that of two permutations — is the operation of *function composition*. It is this second operation — function composition — that mathematicians have in mind when speaking of permutation products today.

The *product* of a given arrangement xyz by a permutation $\begin{pmatrix} xyz \\ xzy \end{pmatrix}$ is the new arrangement xzy which is obtained by applying this same substitution to the given arrangement. The *product* of two permutations will be the new permutation that always furnishes, for any arbitrary arrangement, the result obtained by the application of the two [permutations], applied one after the other. The two given permutations are called the two *factors* of the product. The product of an arrangement by a permutation or of a permutation by another [permutation] will be indicated by the [same] notation which serves to indicate the product of two quantities . . . We find, for example,

$$\begin{pmatrix} xyz \\ xzy \end{pmatrix} xyz = xzy$$

and

$$\begin{pmatrix} xyzu \\ yxuz \end{pmatrix} = \begin{pmatrix} xy \\ yx \end{pmatrix} \begin{pmatrix} zu \\ uz \end{pmatrix}$$

There is more; we can, in the second part of the last equation, interchange the two factors with no inconvenience, so that one will have again

$$\begin{pmatrix} xyzu \\ yxuz \end{pmatrix} = \begin{pmatrix} zu \\ uz \end{pmatrix} \begin{pmatrix} xy \\ yx \end{pmatrix}.$$

But this interchange will not always be possible, and the product of two permutations will often vary when the two factors are interchanged. Thus, in particular, we will find

$$\begin{pmatrix} xy \\ yx \end{pmatrix} \begin{pmatrix} yz \\ zy \end{pmatrix} = \begin{pmatrix} xyz \\ yzx \end{pmatrix} \qquad \begin{pmatrix} yz \\ zy \end{pmatrix} \begin{pmatrix} xy \\ yx \end{pmatrix} = \begin{pmatrix} xyz \\ zxy \end{pmatrix}$$

We will say that two permutations *commute*, when their product is independent of the order in which the two factors occur.

To verify the products in Cauchy's illustration of the non-commutative nature of permutation multiplication, remember that each 'product' is really a composition function with $(g \circ f)(z) = g(f(z))$. To compute the product of permutations, therefore, we must begin with the *right* most factor (or function), and then move to the left. For example, to determine where z is mapped by the product $\begin{pmatrix} xy \\ yx \end{pmatrix} \begin{pmatrix} yz \\ zy \end{pmatrix}$, we

first look at the effect of the (right-most) permutation $\begin{pmatrix} yz \\ zy \end{pmatrix}$ on the input z, finding that z is mapped to y. We then use y as our input and look at how it is transformed by the (left-most) permutation $\begin{pmatrix} xy \\ yx \end{pmatrix}$, finding that y is mapped to x. We conclude that z is mapped to x by the product permutation, as is indeed the case in Cauchy's example: $\begin{pmatrix} xy \\ yx \end{pmatrix}\begin{pmatrix} yz \\ zy \end{pmatrix} = \begin{pmatrix} xyz \\ yzx \end{pmatrix}$.

Task 2

(a) By tracing the effect each factor has on individual variables, moving from right to left, explain why x is mapped to y and why y is mapped to z by the product $\begin{pmatrix} xy \\ yx \end{pmatrix}\begin{pmatrix} yz \\ zy \end{pmatrix}$. This completes the verification of the first half of Cauchy's illustration.

(b) Verify the second half of Cauchy's illustration: $\begin{pmatrix} yz \\ zy \end{pmatrix}\begin{pmatrix} xy \\ yx \end{pmatrix} = \begin{pmatrix} xyz \\ zxy \end{pmatrix}$.

(c) Compute and compare the two products $\begin{pmatrix} xyu \\ uxy \end{pmatrix}\begin{pmatrix} xzu \\ zux \end{pmatrix}$ and $\begin{pmatrix} xzu \\ zux \end{pmatrix}\begin{pmatrix} xyu \\ uxy \end{pmatrix}$.

Write each in the form $\begin{pmatrix} x\,y\,z\,u \\ *\,*\,*\,* \end{pmatrix}$.

(d) Compute and compare the two products $\begin{pmatrix} xyu \\ uxy \end{pmatrix}\begin{pmatrix} zvw \\ wvz \end{pmatrix}$ and $\begin{pmatrix} zvw \\ wvz \end{pmatrix}\begin{pmatrix} xyu \\ uxy \end{pmatrix}$.

Write each in the form $\begin{pmatrix} x\,y\,z\,u\,v\,w \\ *\,*\,*\,*\,*\,* \end{pmatrix}$.

(e) Based on Cauchy's examples and parts (c) and (d) of this task, what conjectures, if any, do you have about permutations that commute? Explain your reasoning.

Task 3 Recall that function composition is associative, so that $(f \circ g) \circ h = f \circ (g \circ h)$. Accordingly, permutation multiplication is also associative. Verify this in the following particular case by computing the product below in the two ways indicated:

(a) $\left[\begin{pmatrix} xyzu \\ yxzu \end{pmatrix}\begin{pmatrix} xyzu \\ zxuy \end{pmatrix}\right]\begin{pmatrix} xyzu \\ uxyz \end{pmatrix}$ (b) $\begin{pmatrix} xyzu \\ yxzu \end{pmatrix}\left[\begin{pmatrix} xyzu \\ zxuy \end{pmatrix}\begin{pmatrix} xyzu \\ uxyz \end{pmatrix}\right]$

Task 4 Cauchy sometimes used indexed letters $x_1, x_2, \ldots$ to denote the objects being permuted. Clearly, this does not affect how permutation products are computed, but only how much writing we do and how easy it is to read the results. To see this, compute the following:

$$\begin{pmatrix} x_1\,x_2\,x_3\,x_4\,x_5 \\ x_3\,x_1\,x_2\,x_5\,x_4 \end{pmatrix}\begin{pmatrix} x_1\,x_2\,x_3\,x_4\,x_5 \\ x_5\,x_4\,x_2\,x_3\,x_1 \end{pmatrix}$$

How might we denote permutations involving indexed letters more concisely?

1.2 Permutation Order

In our next two excerpts from Cauchy, the results of multiplying a permutation by itself are explored. The commentary and project tasks interspersed between and following these two excerpts will elaborate on the details of Cauchy's arguments. Note that Cauchy has used i to denote a natural number, *not* the imaginary square root of -1. Also remember that '1' represents the multiplicative identity for permutations.

Nothing is lost if we represent the arrangements formed by several variables by simple letters

$$A, B, C, \ldots$$

or by letters affixed with indices

$$A_1, A_2, A_3, \ldots.$$

Then the permutation which has for its terms A and B will be simply represented in the form

$$\begin{pmatrix} A \\ B \end{pmatrix} \ldots$$

The total number of permutations relative to a system of n variables ... will evidently be equal to the number N of arrangements that can be formed with these variables. ... The permutation for which the numerator and the denominator are the same, can be supposed to reduce to unity, since one can evidently replace it by the factor 1 in products:

$$\begin{pmatrix} A \\ A \end{pmatrix} C = C, \qquad \begin{pmatrix} A \\ A \end{pmatrix} \begin{pmatrix} C \\ D \end{pmatrix} = \begin{pmatrix} C \\ D \end{pmatrix}.$$

A permutation $\begin{pmatrix} A \\ B \end{pmatrix}$, multiplied by itself several times in a row, gives for successive products its *square*, its *cube*, and generally its different *powers*, which are naturally represented by the notation

$$\begin{pmatrix} A \\ B \end{pmatrix}^2, \begin{pmatrix} A \\ B \end{pmatrix}^3, \begin{pmatrix} A \\ B \end{pmatrix}^4 \ldots,$$

can never include more than N actually distinct permutations. Therefore, in extending this series, we will eventually see the same permutations.[12]

[12] Cauchy's argument for this fact is based on the so-called 'Pigeonhole Principle.' With only a finite number ($N = n!$) of different values possible for all the infinitely many powers of $\begin{pmatrix} A \\ B \end{pmatrix}$, some two of these powers (pigeons) must share the same value (hole). That is, there must be some $h \neq l$ such that $\begin{pmatrix} A \\ B \end{pmatrix}^h = \begin{pmatrix} A \\ B \end{pmatrix}^l$.

What's more, if we suppose that

$$\begin{pmatrix} A \\ B \end{pmatrix}^h = \begin{pmatrix} A \\ B \end{pmatrix}^l,$$

h being $< l$, then, in setting, as an abbreviation,

$$l = i + h$$

we will have[13]

$$\begin{pmatrix} A \\ B \end{pmatrix}^h = \begin{pmatrix} A \\ B \end{pmatrix}^l = \begin{pmatrix} A \\ B \end{pmatrix}^{i+h} = \begin{pmatrix} A \\ B \end{pmatrix}^i \begin{pmatrix} A \\ B \end{pmatrix}^h,$$

consequently

$$\begin{pmatrix} A \\ B \end{pmatrix}^i = 1,$$

i being evidently less than l.

The central objective of the excerpt we have just read was to prove that for every permutation $\begin{pmatrix} A \\ B \end{pmatrix}$, there exists a natural number $i \leq N$ for which $\begin{pmatrix} A \\ B \end{pmatrix}^i = 1$, where $N = n!$ is the number of all distinct permutations. Task 5 explores the property which defines the number i for a given permutation, while Task 6 further examines Cauchy's proof of the existence of such a number for any permutation.

Task 5 Letting $\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} xyzu \\ uxyz \end{pmatrix}$, compute powers of $\begin{pmatrix} A \\ B \end{pmatrix}$ to determine the *smallest* natural number i for which $\begin{pmatrix} A \\ B \end{pmatrix}^i = 1$. *(Since there are* $4! = 24$ *different permutations of* 4 *variables, we know* $i \leq 24$ *. . . hopefully, you won't have to go as far as the* 24^{th} *power!)*

Task 6 In the preceding excerpt, Cauchy derived his conclusion that $\begin{pmatrix} A \\ B \end{pmatrix}^i = 1$ directly from the fact that $\begin{pmatrix} A \\ B \end{pmatrix}^h = \begin{pmatrix} A \\ B \end{pmatrix}^i \begin{pmatrix} A \\ B \end{pmatrix}^h$. Setting $X = \begin{pmatrix} A \\ B \end{pmatrix}^h$ and $Y = \begin{pmatrix} A \\ B \end{pmatrix}^i$, we can rewrite this part of his argument as follows:

$$X = YX \;\Rightarrow\; Y = 1, \text{ where 1 represents the identity.}$$

Although this algebraic property always holds in the case where X, Y are non-zero real or complex numbers, it does not hold in all algebraic structures.

[13] In the interest of clarity, a minor modification has been made in the next line of Cauchy's original text.

(a) Illustrate the failure of this fact in matrix algebra by showing that we have $X = YX$ with $X \neq 0$ and $Y \neq I$ (where I is the 2×2 identity matrix) for the following specific matrices:

$$X = \begin{bmatrix} 0 & 0 \\ 0 & 7 \end{bmatrix} \quad \text{and} \quad Y = \begin{bmatrix} 2 & 0 \\ 3 & 1 \end{bmatrix}.$$

(b) Now let X, Y be permutations and suppose $X = YX$. According to Cauchy's argument, this is sufficient to conclude, without further ado, that Y must be the identity permutation in this case. Write as convincing an argument as you can to justify this conclusion, based only on what you already know about how permutations behave.

We now look at the continuation of the preceding excerpt, where we will see Cauchy's argument that the powers of $\begin{pmatrix} A \\ B \end{pmatrix}$ behave periodically, in a fashion reminiscent of how sets of roots of unity behave.[14] Notice that Cauchy's proof of the periodicity of powers of permutations starts from the (already established) fact that there exists a power i with $\begin{pmatrix} A \\ B \end{pmatrix}^i = 1$. Be sure that you can justify each step of the argument that follows from there as you read through it.

There is more; if, taking i to be the value determined by the preceding formula, we let l be an arbitrary whole number, k the quotient when l is divided by i, and j the remainder of this division, so that we have

$$l = ki + j,$$

j being less than i, we will find not only that

$$\begin{pmatrix} A \\ B \end{pmatrix}^{ki} = \left[\begin{pmatrix} A \\ B \end{pmatrix}^{i}\right]^k = 1^k = 1,$$

but, furthermore, that

$$\begin{pmatrix} A \\ B \end{pmatrix}^{l} = \begin{pmatrix} A \\ B \end{pmatrix}^{ki}\begin{pmatrix} A \\ B \end{pmatrix}^{j} = \begin{pmatrix} A \\ B \end{pmatrix}^{j},$$

and, examining the former formula in the case where the number k is reduced to zero, we will also

[14] Recall that an m^{th} root of unity is a solution of the equation $x^m = 1$, where there are m such solutions within the set of complex numbers. Geometrically, nineteenth-century mathematicians were already accustomed to thinking of these m roots as m equally-spaced points on the unit circle, with $x = 1$ always one of these points. Algebraically, as was also well-known prior to the work of Cauchy, these m solutions are given by the formula $x = e^{\frac{\pi k}{m} i}$, $k = 1, 2, \ldots, m$, where $e^{\frac{k\pi}{m} i} = \cos\left(\frac{k\pi}{m}\right) + i \sin\left(\frac{k\pi}{m}\right)$ by De Moivre's Theorem. It was also known by that time that certain roots of unity,for example the 'first' such root, $x = e^{\frac{\pi}{m} i}$, are capable of producing all m^{th} roots of unity by taking its powers. [For $x = e^{\frac{\pi}{m} i}$, this is easy to prove since $\left(e^{\frac{\pi}{m} i}\right)^k = e^{\frac{k\pi}{m} i}$.] Roots of this kind are known as *primitive* roots of unity.

have

$$\begin{pmatrix} A \\ B \end{pmatrix}^0 = 1$$

In virtue of these remarks that we have just made, if we prolong indefinitely the series whose terms are

$$\begin{pmatrix} A \\ B \end{pmatrix}^0 = 1\,,\ \begin{pmatrix} A \\ B \end{pmatrix}\,,\ \begin{pmatrix} A \\ B \end{pmatrix}^2\,,\ \begin{pmatrix} A \\ B \end{pmatrix}^3\,,\ \text{etc}\ldots,$$

the unity [1] will be the first of these terms that will be repeated, and from there the rest of the terms already found will reappear periodically in the same order, so that one will have, for example

$$1 \quad = \quad \begin{pmatrix} A \\ B \end{pmatrix}^i \quad = \quad \begin{pmatrix} A \\ B \end{pmatrix}^{2i} \quad = \quad \ldots,$$

$$\begin{pmatrix} A \\ B \end{pmatrix} \quad = \quad \begin{pmatrix} A \\ B \end{pmatrix}^{i+1} \quad = \quad \begin{pmatrix} A \\ B \end{pmatrix}^{2i+1} \quad = \quad \ldots,$$

$$\begin{pmatrix} A \\ B \end{pmatrix}^2 \quad = \quad \begin{pmatrix} A \\ B \end{pmatrix}^{i+2} \quad = \quad \begin{pmatrix} A \\ B \end{pmatrix}^{2i+2} \quad = \quad \ldots,$$

$$\text{etc.} \quad \ldots$$

Therefore the number i of distinct terms of the series will always be the smallest natural number value of i which satisfies the formula

$$\begin{pmatrix} A \\ B \end{pmatrix}^i = 1$$

The number i thereby determined, or the degree of the smallest power of $\begin{pmatrix} A \\ B \end{pmatrix}$ equivalent to the identity, is what we will call the degree or the *order* of the permutation $\begin{pmatrix} A \\ B \end{pmatrix}$.

Cauchy's definition of the ***order of a permutation*** P as the least positive integer i with $P^i = 1$ is still used today. For an example illustrating this concept, look back at Task 5, where you should have found that $i = 4$ is the *smallest* natural number for which $\begin{pmatrix} xyzu \\ uxyz \end{pmatrix}^i = 1$. This means that 4 is the order of the permutation $\begin{pmatrix} xyzu \\ uxyz \end{pmatrix}$.

Task 7 Compute powers of the following permutations to determine the order of each.

(a) $\begin{pmatrix} xyzu \\ zxyu \end{pmatrix}$ (b) $\begin{pmatrix} xyzu \\ xzyu \end{pmatrix}$ (c) $\begin{pmatrix} xyzuv \\ zxyvu \end{pmatrix}$

1.3 Cycles and Transpositions

As you have been computing products and powers of permutations, you may have noticed that some permutations behave simply by cycling through all the variables in a particular order, as in the case of $\begin{pmatrix} xyzu \\ uxyz \end{pmatrix}$, where we have $x \to u \to z \to y \to x$. Other permutations have more complicated behavior, but still exhibit this sort of cyclic behavior on various subsets of their variables; for example, the permutation $\begin{pmatrix} xyzuv \\ zxyvu \end{pmatrix}$ could be thought of as two separate cycles: $x \to z \to y \to x$ and $u \to v \to u$. In our next excerpt, Cauchy's terminology and notation for permutations with this behavior is introduced.

We now suppose that a permutation reduced to its simplest expression has the form

$$\begin{pmatrix} xy \ldots uvw \\ yz \ldots vwx \end{pmatrix}$$

that is to say that it operates by replacing x by y, then y by z, ..., and so in succession until the final variable w is reached, which is replaced by the variable x with which we began. To carry out this permutation, we can arrange the different variables,

$$x, y, z, \ldots, u, v, w,$$

on the circumference of an *indicator* circle, divided in equal parts, placing the first, the second, the third, ... [variable] on the first, the second, the third, ... point of the division, then to replace every variable with that which comes to take its place when we turn the indicator circle in a certain direction. For this reason we give the permutation in question the name *circular permutation*. We will represent it, as an abbreviation, by the notation

$$(x, y, z, \ldots, u, v, w);$$

and it is clear, in this notation, that any one of the variables

$$x, y, z, \ldots, u, v, w$$

can occupy the first place. Thus, for example, we have the identity

$$(x, y, z) = (y, z, x) = (z, x, y).$$

Today, we use the (shorter) term ***cycle*** for what Cauchy called a *circular permutation*. Although many current texts also omit the commas between elements in a cycle as a notational abbreviation, we follow Cauchy's convention in this regard in the remainder of this project.

Task 8 Which of the following cycles are equal? Justify your answer.

$$(x,\, y,\, z,\, u,\, v) \quad ; \quad (y,\, z,\, v,\, x,\, u) \quad ; \quad (z,\, u,\, v,\, x,\, y) \quad ; \quad (u,\, z,\, x,\, y,\, v) \quad ; \quad (v,\, x,\, u,\, y,\, z)$$

Our next excerpt from Cauchy gives a simple rule for finding the order of a cycle. We omit Cauchy's argument for this rule, which involved examining how far the 'indicator circle' must be turned in order to return all the variables to themselves. You should, however, be able to convince yourself of the truth of the rule he gives simply by thinking about the nature of cycles. Cauchy also gave two examples to illustrate the fact that his rule for the order of a cycle gives the same result as would be obtained by taking powers of the cycle until we arrive at the identity; the first of his examples is included in this excerpt and further examined in Task 9; the second of his examples is considered in Task 10.

If we call i the number of variables included in a circular permutation

$$(x, y, z, \ldots, u, v, w),$$

then ..... the order of a circular permutation will be exactly the number i of letters that it contains.

...

If, to fix these ideas, we let $i = 4$, then, in raising the circular permutation

$$(x,\, y,\, z,\, u),$$

to the second and to the third power, we would find

$$(x,\, y,\, z,\, u)^2 = (x,\, z)(y,\, u) \qquad , \qquad (x,\, y,\, z,\, u)^3 = (x,\, u,\, z,\, y)$$

.

Referring to a cycle that involves exactly i letters as an ***i*-cycle**, Cauchy has just claimed that every i-cycle has order i. In addition to further exploring this claim, the next two tasks direct our attention to similarities in the behavior of an i-cycle and that of a primitive i^{th} root of unity. (See footnote 14 for some reminders about roots of unity.)

Task 9 Consider the 4-cycle $\beta = (x,\, y,\, z,\, u)$.

(a) Verify Cauchy's claims in the preceding excerpt that $\beta^2 = (x,\, z)(y,\, u)$ and that $\beta^3 = (x,\, u,\, z,\, y)$. Then verify that $\beta^4 = 1$, either by computing $\left[\beta^2\right]^2$ or by computing $\beta^3\beta$. Explain why this confirms that any arbitrary 4-cycle will have order 4.

(b) Note that the permutation $\beta^3 = (x,\, u,\, z,\, y)$ is also a 4-cycle and thus has order 4. Determine the order of the permutation $\beta^2 = (x,\, z)(y,\, u)$, and justify your answer.

(c) Compare the set $\{\beta, \beta^2, \beta^3, 1\}$ with the set $\{i, -1, -i, 1\}$ of 4^{th} roots of unity .

Task 10 Consider an arbitrary 6-cycle $\beta = (x,\, y,\, z,\, u,\, v,\, w)$.

(a) Compute the permutations β^k for $k = 2, 3, 4, 5, 6$ to confirm that β has order 6.

(b) Which of the permutations β^k, other than β itself, also have order 6? Justify.

(c) What is the order of the permutations β^k which are not of order 6? Justify.

(d) Compare the set $\{\beta, \beta^2, \beta^3, \beta^4, \beta^5, 1\}$ with the set $\{e^{\frac{\pi}{6}i}, e^{\frac{\pi}{3}i}, -1, e^{\frac{2\pi}{3}i}, e^{\frac{5\pi}{6}i}, 1\}$ of 6^{th} roots of unity.

From your work in the previous two tasks, it should be clear that the power of a cycle can be a product of two or more cycles, rather than just a single cycle. For instance, for $\beta = (x,\, y,\, z,\, u)$, we have $\beta^2 = (x,\, z)(y,\, u)$. Notice also that none of the elements in these factors overlap; in other words, the cycles that appear as factors in this product are ***disjoint***. In the following excerpt, Cauchy explained that every permutation can be written as the product of disjoint cycles in this way. We call this product the ***cycle decomposition*** of the permutation β. As you continue reading, keep the question of whether a cycle decomposition is necessarily unique (up to the order of the factors) in mind.

Now let A and B be two arbitrary arrangements formed with n variables $x, y, z, \ldots$. To substitute the second arrangement for the first, it will evidently suffice to operate with one or several circular permutations [cycles], that can be readily formed by placing two variables in the order in which the one will be replaced by the other when we pass from the first arrangement to the second. Consequently, the permutation, reduced to its simplest expression, will necessarily be either a circular permutation [cycle], or the product of several circular permutations [cycles]. We find, for example, ...

$$\begin{pmatrix} xyzu \\ uzyx \end{pmatrix} = (x,\, u)(y,\, z) \qquad , \qquad \begin{pmatrix} xyzuv \\ zuvyx \end{pmatrix} = (x,\, z,\, v)(y,\, u)$$

The circular permutations [cycles] of which the arbitrary permutation $\begin{pmatrix} A \\ B \end{pmatrix}$ will be the product are called the *cyclic factors* of $\begin{pmatrix} A \\ B \end{pmatrix}$. Any arbitrary two of these [cyclic factors], being composed of distinct letters, will clearly commute. Thus, all the cyclic factors of a permutation commute with each other, and will represent the permutation in question in any order.

You may already have noticed that disjoint cycles necessarily commute, as noted above by Cauchy. Look back, for example, at your explorations in Task 2, especially part (e). You may also have remarked how useful the commutativity of disjoint cycles can be when computing products or powers. Representing a permutation by its cycle decomposition allows us to take full advantage of this. For example, using commutativity of disjoint cycles, together with associativity of permutation products, we know that

$$[(x,\, u)(y,\, z)]\,[(x,\, u)(y,\, z)] = [(x,\, u)(x,\, u)]\,[(y,\, z)(y,\, z)]\,,$$

so that

$$\begin{pmatrix} xyzu \\ uzyx \end{pmatrix}^2 = [(x,\, u)(y,\, z)]^2 = (x,\, u)^2(y,\, z)^2 = 1$$

Note that this also shows that the permutation $\begin{pmatrix} xyzu \\ uzyx \end{pmatrix}$ has order 2.

Task 11 Use the fact that disjoint cycles commute to simplify computations in this task.
[*Remember that multiplication of permutations in general is not commutative!*]

(a) Explain why the following permutation has order 2: $\alpha = \begin{pmatrix} xyzu \\ zuxy \end{pmatrix} = (x,\, z)(y,\, u)$

(b) Explain why the following permutation has order 2: $\beta = \begin{pmatrix} xyzuvw \\ zuxyvw \end{pmatrix} = (x,\, z)(y,\, u)(v,\, w)$

(c) Find the order of the following permutation and justify. $\gamma = \begin{pmatrix} xyzuvw \\ zxyvwu \end{pmatrix} = (x,\, z,\, y)(u,\, v,\, w)$

Task 12 Consider the permutation $\alpha = \begin{pmatrix} xyzuv \\ zuvyx \end{pmatrix} = (x,\, z,\, v)(y,\, u)$

(a) Make a conjecture concerning the order of the permutation α; explain why you think this will be correct based on what we know about the order of cycles.

(b) Find the order of α by computing its powers until the identity 1 is reached.
Use the fact that disjoint cycles commute to simplify the computation.
[*Remember that multiplication of permutations in general is not commutative!*]

(c) Was your conjecture in part (a) correct? If not, how would you modify it?

Task 13 Products of disjoint cycles are just one representational form for permutations studied by Cauchy; this task begins to explores another such product decomposition which remains important today. Further explorations of this idea appear in Task 17.

We will say that a permutation P is a ***transposition*** if and only if P is a 2-cycle.[15]

Note that a 3-cycle can be written as the product of transpositions in (at least) two ways:

$$(x_1\,,\, x_2\,,\, x_3) = (x_1\,,\, x_2)(x_2\,,\, x_3) \qquad \textit{and} \qquad (x_1\,,\, x_2\,,\, x_3) = (x_1\,,\, x_3)(x_1\,,\, x_2)$$

Also note that both decompositions involve exactly two transpositions.
Although it is not possible to decompose a 3-cycle into fewer than two transpositions, it can be done with more; for example, $(x_1\,,\, x_2\,,\, x_3) = (x_1\,,\, x_2)(x_3\,,\, x_1)(x_1\,,\, x_3)(x_2\,,\, x_3)$.

(a) Using as few transpositions as possible, write the general 4-cycle $(x_1\,,\, x_2\,,\, x_3\,,\, x_4)$ as the product of transpositions in at least two different ways.

[15] Cauchy introduced this definition in his earliest works on permutation theory.

(b) Using as few transpositions as possible, write the general n-cycle $(x_1, x_2, \ldots, x_n)$ as the product of transpositions in two different ways.

(c) Explain how to write an arbitrary permutation P as the product of transpositions. Don't forget that the identity 1 is also a permutation!

1.4 Permutation Inverses and More

Before we turn to Cauchy's writing on systems of permutations in the next section, we need one more algebraic idea related to individual permutations, that of an ***inverse permutation***. Cauchy wrote about inverses in several sections of his 1845 manuscript; in the next excerpt, we have selected only those of his comments which are relevant to our immediate purposes of this project.

∞∞

It is good to observe that if, after substituting for the arrangement A another arrangement B, we wish to return from the arrangement B to the arrangement A, this second operation, the inverse of the first, will be represented not by the notation $\begin{pmatrix} A \\ B \end{pmatrix}$, but by the notation $\begin{pmatrix} B \\ A \end{pmatrix}$. Consequently, it is natural to say that the two permutations

$$\begin{pmatrix} A \\ B \end{pmatrix}, \quad \begin{pmatrix} B \\ A \end{pmatrix}$$

are *inverses* of each other. That said, it is clear that, if the permutation which puts in the place of x another variable y, the inverse permutation will put, oppositely, y in the place of x. ...

....

...[I]f we let $P = \begin{pmatrix} A \\ B \end{pmatrix}$, then P^{-1} will be the permutation which, when multiplied by $\begin{pmatrix} A \\ B \end{pmatrix}$, will have as its product 1; that is to say, the permutation $\begin{pmatrix} B \\ A \end{pmatrix}$, inverse of $\begin{pmatrix} A \\ B \end{pmatrix}$. Thus, the notations

$$P, P^{-1}$$

designate in general two permutations which are inverses of each other.

∞∞

It is perhaps important to remark here that the excerpt you have just read omits the algebraic argument which Cauchy gave concerning why it makes sense to denote the inverse of a permutation P by the (negative) power P^{-1}. You are, of course, already familiar with this notation for inverse functions from calculus.[16] The general algebraic identity $P^{-1}P^1 = P^{-1+1} = P^0 = 1$, which is more in keeping with Cauchy's actual argument in favor of this notation, will also be familiar to you.

What may be less familiar is the process of actually finding the inverse of a given permutation. In the first part of this excerpt, Cauchy suggested that one way to find the inverse of the permutation $P = \begin{pmatrix} A \\ B \end{pmatrix}$

[16]Since a permutation is really a one-to-one onto function, it necessarily has an inverse function.

is to simply reverse the two rows, to get $P^{-1} = \begin{pmatrix} B \\ A \end{pmatrix}$.

For example, if we let

$$P = \begin{pmatrix} xyzu \\ yzux \end{pmatrix}$$

then

$$P^{-1} = \begin{pmatrix} yzux \\ xyzu \end{pmatrix}.$$

If this last permutation looks somehow disarranged to you, it is only because we have been writing the top row as '$xyzu$' in this project; putting the variables of the top row back in the order we have come to expect them and moving the corresponding variables in the bottom row along with them, we get

$$P^{-1} = \begin{pmatrix} y & z & u & x \\ | & | & | & | \\ x & y & z & u \end{pmatrix} = \begin{pmatrix} x & y & z & u \\ | & | & | & | \\ u & x & y & z \end{pmatrix} = \begin{pmatrix} xyzu \\ uxyz \end{pmatrix}$$

Finding inverses of cycles is particularly easy, since we can simply reverse the order, as shown here:

$$P = \begin{pmatrix} xyzu \\ yzux \end{pmatrix} = (x,\, y,\, z,\, u) \quad \Rightarrow \quad P^{-1} = (x,\, y,\, z,\, u)^{-1} = (u,\, z,\, y,\, x) = (x,\, u,\, z,\, y)$$

There are other procedures for finding the inverse of a permutation as well. However, the actual procedure for doing this is less important than the general algebraic concept involved; namely, for every permutation P, there is a unique permutation P^{-1} for which $PP^{-1} = P^{-1}P = 1$. Using this concept, for instance, allows us to easily prove that the equation $XY = X$ implies $Y = 1$ in permutation theory by simply multiplying both sides of the equation $X = XY$ on the left by X^{-1}. (*Do you see why it is important to use *left* multiplication here?*) To more fully appreciate the (algebraic) power offered by the existence of inverses, you may wish to compare this proof to the one which you gave for this same fact in Task 6(b). The next task illustrates also the (algebraic) power offered by the uniqueness of inverses.

Task 14 Let P be a permutation of order i, where $i \in \mathbb{Z}^+$. Use the fact that inverse permutations are unique to show that $P^{-1} = P^{i-1}$.

The remaining tasks in this subsection provide some computational practice with permutations inverses and cycle decompositions.

Task 15 (a) Find the inverse of the following permutations without resorting to cycle notation.

(i) $R = \begin{pmatrix} xyzuv \\ zxvuy \end{pmatrix}$ **(ii)** $S = \begin{pmatrix} xyzuv \\ zuvyx \end{pmatrix}$

(b) Find the inverse of the following cycles.

(i) $T = (z,\, y,\, x)$ (ii) $U = (u,\, v,\, y,\, x,\, z)$

Task 16 In matrix theory, we know that $(MN)^{-1} = N^{-1}M^{-1}$, where M, N are invertible matrices.

(a) Explain why this product inverse rule also holds when M, N are permutations.
Hint: Look at $[MN][N^{-1}M^{-1}]$ and $[N^{-1}M^{-1}][MN]$.

(b) Give an example to show that $(MN)^{-1} = M^{-1}N^{-1}$ may fail to hold for permutations.

(c) Use the rule $(MN)^{-1} = N^{-1}M^{-1}$ to compute the inverses of each of the following. Then write each result as a product of disjoint cycles.

(i) $P = (x,\, u,\, z,\, y)(x,\, s,\, y)$ **(ii)** $Q = (s,\, z,\, y,\, u)(x,\, t,\, u)(s,\, x)$

(d) Compute the inverse of each of the following by first writing the given permutation as the product of disjoint cycles, and then inverting.

(i) $P = (x,\, u,\, z,\, y)(x,\, s,\, y)$ (ii) $Q = (s,\, z,\, y,\, u)(x,\, t,\, u)(s,\, x)$

Why is it no longer strictly necessary (but perhaps advisable) to use the permutation product inverse rule $(MN)^{-1} = N^{-1}M^{-1}$ as part of this method?

(e) Which of the inverse methods used in parts (c) and (d) do you prefer, and why?

(f) Find the inverses of each of the following by first writing the given permutations as products of disjoint cycles.

(i) $R = \begin{pmatrix} xyzuv \\ zxvuy \end{pmatrix}$ (ii) $S = \begin{pmatrix} xyzuv \\ zuvyx \end{pmatrix}$

Compare your results to those you obtained in Task 15(a).
Comment on which method of finding inverses you prefer, and why.

Task 17 This task continues the exploration of transposition decompositions begun in Task 13.

Recall from that task that 'transposition' is another term for a 2-cycle.
Also recall that every permutation can be decomposed into transpositions in multiple ways.

We will say that a permutation is ***even*** (***odd***) if it can be written as the product of an even (odd) number of transpositions.

For example, since every 3-cycle can be written as the product of two transpositions (as shown in Task 13), all 3-cycles are even permutations.

(a) Show that the identity permutation 1 is an even permutation.

(b) Use your findings from Task 13 to explain why an n-cycle is even if and only if n is odd.

(c) Let P be an arbitrary permutation. Show that P^{-1} is even if and only if P is even.

(d) Although we will not do so here, it is straightforward to prove that the identity permutation can *only* be written as the product of an even number of transpositions. This implies that the identity permutation itself is not both even and odd.

Use the fact that the identity permutation 1 can *only* be written as the product of an even number of permutations to write a careful proof (by contradiction) that no permutation is both even and odd. Begin by assuming P is a permutation which can be written as the product of an even number of transpositions. and also as the product of an odd number of transpositions. Then consider the product PP^{-1}.

2 'Systems of conjugate permutations' in Cauchy's theory

Up to this point in his manuscript, Cauchy was considering just one or two permutations at a time. In this subsection, we turn to excerpts in which he considered *sets* of permutations formed in a particular way. The resulting structure, which Cauchy called a 'system of conjugate permutations,' is equivalent to what is today called a *permutation group* or a *group of permutations*.[17] We say more about today's notation for permutation groups at the end of Subsection 2.2. In our excerpts from Cauchy, however, we use his term 'system of conjugate permutations' and his notation in recognition of the fact that the general group concept had not yet emerged at the time he did his work.

Being given one or several permutations which contain n letters $x, y, z, \ldots$ or at least several of these, I will call *derived* permutations all those [permutations] which can be generated from multiplying the one or more of the given permutations, by each other or by themselves, in any arbitrary order; and the given permutations, joined [together] with the derived permutations, will form what I call *a system of conjugate permutations*. The *order* of the system will be the total number of permutations present, including the [identity] permutation which ... reduces to unity.

When only a single permutation P is given, the derived permutations are the powers of P and form a system of conjugate permutations which has the same order as that of the permutation P.

Let us pause in our reading to consider some examples. Suppose we are given the two permutations

$$P = (x,\, y) \text{ and } Q = (z,\, u).$$

The *derived permutations* here will include all permutations obtained by multiplying P and Q by themselves and with each other, perhaps repeatedly; in general, this will include products like PQ, QP, P^2, Q^2, P^2Q, PQP, QPQ, QP^2QP, P^3, and so on. In this particular example, however, we know that $P^2 = 1$, $Q^2 = 1$ and $PQ = QP$; thus, all these variations reduce to just four *derived permutations*:

$$1\ ,\ P = (x,\, y)\ ,\ Q = (z,\, u)\ \text{ and }\ PQ = (x,\, y)(z,\, u).$$

The *system of conjugate permutations* in this example, which consists of all the given permutations together with all derived permutations, is therefore the following set:[18]

$$\{1\,,\, P\,,\, Q\,,\, PQ\}.$$

Since this set has four elements, we will say (as did Cauchy) that this system has order 4. Notice too that this set is ***closed under products***; that is, the product of any two of the permutations in this set is also in the set. You should convince yourself that this is the case for any system of conjugate permutations (i.e., permutation group), in light of how such a system is formed by collecting together all possible products formed from the given permutations.

[17] In group theory today, there is a concept called a 'conjugate' which is related to some of Cauchy's work on permutations, but not directly related to his use of the term here; we will not consider the modern concept in this project.

[18] Since permutations on finite sets of variables will always have finite order, the given permutations will also be considered derived permutations. This is not true for permutations on infinite sets, but this case was not considered by Cauchy. Thus, it is unclear why he distinguished between the set of derived permutations and the system of conjugate permutations since these sets are the same in all his examples.

Task 18 Suppose we are given the two permutations $P = (x,\ y,\ z)$ and $Q = (u,\ v)$.

(a) Explain why the *derived permutations* have the form $P^k Q^m$, where $k = 1, 2, 3$ and $m = 1, 2$, so that the *system of conjugate permutations* generated by P, Q is the set

$$\{\, 1\,,\ P\,,\ P^2\,,\ Q\,,\ PQ\,,\ P^2Q\,\}$$

Conclude that the system of conjugate permutations in this example has order 6.

(b) Show that this system is ***closed under inverses***; that is, for every permutation in the system, show that its inverse is also in the system.

(c) Show this system includes two permutations of order 6, two permutations of order 3, and one permutation of order 2. Compare this to the 6^{th} roots of unity. (See footnote 14 and Task 10(d).)

Task 19 Suppose we are given just the one permutation $P = (x,\ y,\ z,\ u,\ v,\ w)$.

(a) Explain why the system of conjugate permutations in this example has order 6.

(b) Show that this system is closed under inverses. (See Task 18(b) for a definition.)

(c) Determine the order of each of the six permutations in this system.
How does this compare to what happens with the system in Task 18?

Task 20 Suppose we are given the two permutations $P = (x,\ y)$ and $Q = (x,\ z)$.
Note that P and Q are *not* disjoint cycles, and therefore do not commute! However, since $P^2 = 1$ and $Q^2 = 1$, the *derived permutations* all come from the following forms:[19]

$$P, PQ, PQP, PQPQ, PQPQP, \ldots \qquad \text{and} \qquad Q, QP, QPQ, QPQP, QPQPQ, \ldots$$

(a) Show that $PQP = QPQ$ by computing these two permutations.
This means that the list of forms we need to compute is reduced to the following:

$$P, PQ, PQP, PQPQ, PQPQP, \ldots \qquad \text{and} \qquad Q, QP$$

(b) Show that $PQPQ = QP$ by computing these two permutations.
Thus, the list of forms we need to compute is further reduced to the following:

$$P, PQ, PQP \qquad \text{and} \qquad Q, QP$$

(c) Conclude that the system of conjugate permutations in this example has order 6.
List each of the six permutations as a product of disjoint cycles.
Also show that this system is closed under inverses, as this is defined in Task 18(b).

[19] If P instead had order 3, while Q had order 2, we would also need to consider permutations of the forms $P^2\,,\ P^2Q\,;\ P^2QP\,,\ P^2QP^2\,;\ P^2QPQ\,,\ P^2QP^2Q\,;\ P^2QPQP\,,\ P^2QPQP^2\,,\ P^2QP^2QP\,,\ P^2QP^2QP^2\,;\ldots$ and of the forms $Q\,,\ QP^2\,;\ QP^2Q\,;\ QP^2QP\,,\ QP^2QP^2\,;\ QP^2QPQ\,,\ QP^2QP^2Q\ \ldots$.

(d) Show that, unlike the systems in Tasks 18 and 19, none of the individual permutations in this system is of order 6, even though the system itself has order 6.

Note: This shows that, although individual permutations behave in a fashion analogous to a root of unity of the same order as that permutation, a *system* of conjugate permutations may *not* have the same algebraic structure as the set of roots of unity of the same order as the system of conjugate permutations.

We return now to Cauchy's comments on systems of conjugate permutations.

The system of all permutations that one can form with n letters $x, y, z \ldots$ is evidently a system of conjugate permutations. If one names the different arrangements that can be formed with n variables $x, y, z, \ldots$ by

$$A,\, B,\, C, \ldots$$

then the system in question will be

$$(1) \qquad \begin{pmatrix} A \\ A \end{pmatrix},\ \begin{pmatrix} A \\ B \end{pmatrix},\ \begin{pmatrix} A \\ C \end{pmatrix}, \ldots$$

and the number N of these permutations, or the order of the system, will be determined by the formula

$$N = 1.2.3 \ldots n.$$

Now let

$$(2) \qquad 1, P, Q, R \ldots$$

be an arbitrary system of conjugate permutations. According to the very definition of such a system, we will always reproduce the same permutations, only arranged in a different manner, if each of them is multiplied separately by some particular one of them, or if some one of them is multiplied by itself and by the others. Thus, if we let S be some arbitrary one of the permutations in (2), then the distinct terms of the series

$$(3) \qquad S,\, SP,\, SQ,\, SR, \ldots,$$

as well as [the terms] of the series

$$(4) \qquad S,\, PS,\, QS,\, RS, \ldots,$$

are the same as the terms of the series (2) arranged in a new order.

Again we pause in our reading for an example. Consider the system of conjugate permutations of order four consisting of the following permutations:[20]

$$1 \ ,\ \ P = (x,\, y) \ ,\ \ Q = (z,\, u) \ ,\ \ R = (x,\, y)(z,\, u).$$

[20] We looked at this example in the last paragraph on page 19; here, we have set $R = PQ = QP$.

We wish to (left) multiply each term of this system by some one particular permutation (which Cauchy labeled S) in the system. For the sake of specificity, let us take $S = Q = (z,\, u)$. In this case, the resulting series is given by:

$$\underbrace{(z,\, u)}_{S} \;,\; \underbrace{(z,\, u)(x,\, y)}_{SP} \;,\; \underbrace{(z,\, u)(z,\, u)}_{SQ} \;,\; \underbrace{(z,\, u)(x,\, y)(z,\, u)}_{SR}$$

But notice that we also have the following:

$$S = (z,\, u) = Q \qquad\qquad SP = (z,\, u)(x,\, y) = (x,\, y)(z,\, u) = R$$
$$SQ = (z,\, u)(z,\, u) = 1 \qquad\qquad SR = (z,\, u)(x,\, y)(z,\, u) = (x,\, y)(z,\, u)^2 = (x,\, y) = P$$

Thus, the series $S\,,\, SP\,,\, SQ\,,\, SR$ is simply the original system arranged in a new order: $Q\,,\, R\,,\, 1\,,\, P$.

Tasks 21 and 22 provide some additional concrete examples to solidify this idea. But, as Cauchy remarked, it is expected from the very definition of a system of conjugate permutations that we will get the entire original series back. Since a system of conjugate permutations is closed under products, and S is itself a permutation in the system, multiplying any element of the system by S must give us an element of the system. You may be wondering though how we know these products are necessarily distinct — could we somehow end up with $SP = SQ$ for some $P \neq Q$? If so, then only some (not all) of the permutations in the system would be listed in the series S, PS, QS, $RS, \ldots$, and Cauchy's claim would be false. Using what you know about inverses, however, you should be able to convince yourself that $SP = SQ$ can only occur in a system of conjugate permutations when $P = Q$.

Task 21 Consider the example discussed above:

$$1 \;\;,\;\; P = (x,\, y) \;\;,\;\; Q = (z,\, u) \;\;,\;\; R = (x,\, y)(z,\, u).$$

(a) Again letting $S = Q = (z,\, u)$, determine the series S, PS, QS, RS.

Recall from the discussion above that multiplication of the elements $1, P, Q, R$ on the left by S re-ordered these elements in the following way: $Q, R, 1, P$.

Compare this to the order in which the elements $1, P, Q, R$ occur in the series obtained from right multiplication by S.

(b) In general, do you think the original permutations will appear in the same order when left-multiplication is used (e.g., $S, SP, SQ, SR, ST, \ldots$) as when right-multiplication is used (e.g., $S, PS, QS, RS, TS, \ldots$)? Why or why not?

Task 22 Consider the system of conjugate permutations of order 6 from Task 20:

$$1 \;,\; P = (x,\, y) \;,\; Q = (x,\, z) \;,\; R = (x,\, z,\, y) \;,\; S = (y,\, z) \;,\; T = (x,\, y,\, z)$$

(a) Verify that the series S, SP, SQ, SR, S^2, ST gives us all six of the original permutations arranged in a new order.

(b) Verify that the series S, PS, QS, RS, S^2, TS gives us all six of the original permutations arranged in a new order.

(c) Compare the order in which the original permutations appear in the two series found in parts (a) and (b). Would you now change your answer to part (b) of Task 21? Why or why not?

Our final excerpt from Cauchy's comments on systems of conjugate permutations (i.e., permutation groups) gives the proof of an extremely important theorem in group theory. In fact, Arthur Cayley, who is credited with writing the first ever paper on abstact goup theory, used it very early as a concrete example of a group in his landmark paper. Cauchy, of course, was thinking only of permutation groups in his proof. However, his proof strategy works perfectly well for abstract groups, even though it differs somewhat from the proof strategy found in most of today's abstract algebra textbooks. You will encounter the theorem (stated for groups in general) in any current algebra textbook — look for it under the name 'Lagrange's Theorem' — along with a proof reminiscent of Cauchy's approach (but phrased in terms of 'cosets,' a concept discussed briefly later in this project, in footnote 24). Although Lagrange did state a result related to the theorem we are about to see, his work was always done in the (more limited) context of the number of forms resulting from permutations of variables of a function. See [Roth, 2001] for more on the history of this theorem, its proof and how it came to have its current name. We say more about the modern statement of the theorem and its proof below.

You should read (and re-read!) Cauchy's proof of Lagrange's Theorem (for permutation groups) in the following excerpt until you feel that you understand its details. To help with this, you should also read (and re-read!) the comments on Cauchy's proof strategy that we include following this excerpt. In Task 23, you will examine Cauchy's proof strategy in a very specific case, which will further help you to understand his general strategy.

Before reading Cauchy's proof for the first time, recall that he has already introduced the following conventions in the preceding excerpt:

- Series (1) designates the system of *all* possible $N = n!$ permutations on n letters;
- Series (2) designates an arbitrary system of conjugate permutations on n variables, with the individual permutations in the series denoted as $1, P, Q, R \ldots$
- The ***order*** of a system of conjugate permutations is its cardinality as a set.[21]

Theorem 1 The order of a system of conjugate permutations in n variables will always be a divisor of the number of arrangements N that one can form with these variables.

Proof We suppose that the given system is given by the series (2), and we let M be the order of this system. If the series (2) is the same as the series (1), then we have exactly $M = N$; otherwise, we designate by $U, V, W, \ldots$ those permutations which are part of the series (1) but do not appear in the series (2). If we call m the number of terms of the series

$$1, U, V, W, \ldots\ldots \tag{5}$$

then the table

$$\left\{\begin{array}{lllll} 1, & P, & Q, & R, & \ldots \\ U, & UP, & UQ, & UR, & \ldots \\ V, & VP, & VQ, & VR, & \ldots \\ W, & WP, & WQ, & WR, & \ldots \\ \text{etc,} & & & & \end{array}\right. \tag{6}$$

[21] The cardinality of a set is simply the number of elements that it contains.

will give us m horizontal rows each composed of M terms, with all the terms of each row distinct from each other.

If, moreover, two different horizontal rows, for example the second and the third, include equal terms, in which case we would have

$$VQ = UP,$$

we would conclude from this that

$$V = UPQ^{-1}$$

or simply

$$V = US,$$

$S = PQ^{-1}$ being one of the terms of series (2). In this case, the first term V of the third horizontal row in the table (6) would be one of the terms of the second [horizontal rows].

Thus, if the first term of each horizontal row is taken from outside [of all of] the preceding series, all the terms of table (6) will be distinct from each other. Granting that this condition is fulfilled, we continuously add new series to table (6), thereby increasing the number m [of rows]. This operation will stop only when the table (6) includes all N terms contained in the series (1); but then we will evidently have

$$N = mM.$$

Thus, M will be a divisor of N.

Cauchy's basic strategy in his proof of this theorem was to form an m by M array in which every one of the possible $N = n!$ permutations on n letters appears exactly once, and M is the order of the given system of conjugate permutations. The key to doing this is to make sure that:

(i) no row contains repeated elements; and

(ii) no element of a given row appears in some earlier row.

Cauchy really did not say how he knew condition (i) held for all rows in the array, although (i) clearly holds for the first row in which each of the M distinct permutations of the given system are listed exactly once. To convince yourself that condition (i) holds for the other rows, consider what would happen, for example, if $UP = UT$, remembering that $P \neq T$. Concerning condition (ii), Cauchy gave considerably more detail, arguing essentially that careful selection of the first element of each row permits us to successively add new rows containing exactly M elements, all of which are distinct from the elements in every preceding row, until all $N = n!$ possible permutations on n variables are exhausted. Task 23 outlines the construction of a table satisfying these two conditions in a very specific case.

Task 23 This task examines Cauchy's proof of Lagrange's Theorem in a specific example.

Consider the set of all permutations on the four letters x, y, z, u.

From this set, let $H = \{h_1\,,\, h_2\,,\, h_3\,,\, h_4\}$ be the subset consisting of the following:

$$h_1 = 1 \;\;;\;\; h_2 = (x,\, y,\, z,\, u) \;\;;\;\; h_3 = h_2^2 = (x,\, z)(y,\, u) \;\;;\;\; h_4 = h_2^3 = (x,\, u,\, z,\, y)$$

(a) Explain how we know that H is a system of conjugate permutations.

(b) What are the values of N and M in Cauchy's proof for this specific example? Use these values to explain why the completed table should have six rows.

(c) In the partially completed table below a first element (denoted r_2, r_3, r_4 respectively) has been selected for rows 2–4.

(i) Assume for now that the selections made for r_2, r_3, r_4 are valid. WITHOUT COMPUTING ANY ADDITIONAL PRODUCTS, explain why:

(α) $r_4h_3 \neq r_4h_4$ (β) $r_3h_3 \neq r_4h_3$ (γ) $r_4h_3 \neq r_2h_4$

Note: Part (γ) corresponds to the section of Cauchy's proof (beginning with the assumption $VQ = UP$) that shows different rows do not overlap.

(ii) Explain why the particular values chosen for r_2 and r_3 are valid choices.

(iii) Complete row 3, and explain why the particular value chosen for r_4 is valid.

(iv) Complete row 4, and explain why there are eight possible choices for the first entry (r_5) of row 5. Select one of these and explain why your choice is valid. How many possible choices remain for the first entry (r_6) of row 6? (You do not need to complete these last two rows, buy may do so if you wish.)

$h_1 = 1$	$h_2 = (x, y, z, u)$	$h_3 = (x, z)(y, u)$	$h_4 = (x, u, z, y)$
$r_2 = (x, y)$	$r_2h_2 = (x, y)(x, y, z, u)$ $= (y, z, u)$	$r_2h_3 = (x, y)(x, z)(y, u)$ $= (x, z, y, u)$	$r_2h_4 = (x, y)(x, u, z, y)$ $= (x, u, z)$
$r_3 = (x, z)$	$r_3h_2 = (x, z)(x, y, z, u)$ $=$	$r_3h_3 = (x, z)(x, z)(y, u)$ $=$	$r_3h_4 = (x, z)(x, u, z, y)$ $=$
$r_4 = (x, u)$			

(d) Suppose the first element of row 2 in the above table were chosen to be $r_2' = (y, z, u)$, instead of $r_2 = (x, y)$. How would this change the resulting table? Would we have been able to use the same values of r_3, r_4, r_5, r_6 in this case? Why or why not?

Again, you should re-read Cauchy's proof (pages 23–24) along with the comments about it on page 24, and discuss it with others as needed to be sure you understand its details. In Task 24 below, you will be asked re-write Cauchy's proof using the current terminology of permutation groups. The following list explains this terminology and comments on how it is related to that of Cauchy.

- The ***symmetric group*** S_n is the set of all permutations on n objects.[22]
  - This is what Cauchy called (somewhat long-windedly):
    'the system of all permutations that one can form with n letters $x, y, z \ldots$'.
  - In Cauchy's proof of Theorem 1, series (1) lists the elements of S_n.
  - The order of S_n is $n!$.

    Textbooks use different notation to denote the order of a group (or subgroup).
    A common way to do this would be to write: $|S_n| = n!$.

- A ***subgroup of*** S_n is a subset $H \subseteq S_n$ which consists of a collection of given permutations together with all permutations derived from that collection. In other words, a subgroup of S_n is a non-empty subset $H \subseteq S_n$ that is closed under products and, consequently, also closed under inverses.[23]
  - This is what Cauchy called a 'system of conjugate permutations.'
  - In Cauchy's proof of Theorem 1, series (2) lists the elements of a subgroup H.
  - To denote that H is a subgroup of S_n, we write $H \leq S_n$.
  - S_n is always considered a subgroup of itself, since $S_n \subseteq S_n$.

Using this terminology, we now re-state Cauchy's Theorem 1 as follows:

Lagrange's Theorem for the Symmetric Group S_n
If H is a subgroup of S_n, then the order of H divides the order of S_n.

Task 24 Write a fully general rigorous proof of 'Lagrange's Theorem for S_n' using Cauchy's strategy of building an $m \times M$ array in which all $N = n!$ elements of S_n appear exactly once and $M = |H|$ for a given subgroup H. Use the current terminology introduced above. In order to do this in full generality, you should introduce indexed variables to denote the elements of H as well as the first element of each row of the array. (See Task 23.) Then formally (and carefully) use recursion to define the array, and explicitly prove that the completed

[22] The term 'symmetric' in this definition appears to relate back to Lagrange's original analysis of algebraic solvability, where permutations helped to measure the degree to which a given function (for the resolvent's roots) was symmetric.

[23] Closure under inverses follows from closure under products for sets of permutations since $P^{-1} = P^{i-1}$ for any permutation P of order i. However, in the context of more general groups than are treated in this project, the inverse of a group element need not be a power of that element. (*We mention in passing that this means, generally speaking, that group elements need not have finite order. Do you see why not?*) Accordingly, to show that a non-empty set H of a general group G is a subgroup of that group G, we would need to show both closure properties hold (i.e., under products and under inverses).

Note also that a non-empty set H (of permutations or some other elements) that is closed under both products and inverses will necessarily contain the identity 1, since $1 = PP^{-1}$ for any element $P \in H$. Within the context of permutations, this means that once we show a subset H of S_n is non-empty and closed under products, then we know H is also closed under inverses and contains the identity 1. (This last fact actually holds for any *finite* group G (regardless of the nature of its elements) — do you see how to adapt the above arguments to that more general case?)

array satisfies the conditions (i) and (ii) discussed on page 24. Also add detail and/or rephrase Cauchy's reasoning where you feel this is needed and/or helpful.[24]

Task 25 As a corollary to his Theorem 1 (aka, Lagrange's Theorem for the Symmetric Group S_n), Cauchy gave the following result, stated here in the terminology currently in use:

> **Corollary I**
> If H is a subgroup of S_n and P is an arbitrary permutation in H,
> then the order of P divides the order of H.

Cauchy proved Corollary I using an array strategy similar to the one he used to prove Lagrange's Theorem for S_n. Rather than go through the details of this strategy again, this task examines the following somewhat less general corollary:

> **Corollary II**
> For every permutation $P \in S_n$, the order of P divides the order of S_n.

To prove Corollary II directly from Lagrange's Theorem, we only need to find a subgroup H which we know has the same order as the permutation P. The natural candidate for this subgroup H is the set which contains all powers of P; that is, let

$$H = \{\, P^k \mid k \in \mathbb{Z}^+ \,\}.$$

Today, this set H is called the ***cyclic subgroup generated by*** P, denoted $H = \langle P \rangle$.

(a) Explain why H is a subgroup of S_n.

(b) Explain why the order of subgroup H is equal to the order of the permutation P.

(c) Explain why Corollary II now follows from Lagrange's Theorem for S_n.

Task 26 In this task, we examine a special subgroup of S_n, where $n \in \mathbb{Z}^+$ and $n \geq 2$.

Recall from Tasks 13 and 17 that every permutation can be written as the product of transpositions, where a transposition is a 2-cycle.

Also recall that, although this decomposition is not unique, the parity (even versus odd) of the number of transpositions used in the product *is* unique, since a permutation can be written either as the product of an even number of transpositions, or as the product of an odd number of transpositions, but never both. The parity (even or odd) of a permutation is defined to be the parity (even or odd) of this number.

[24] Today's abstract algebra textbooks generally cast the proof of Lagrange's Theorem for a general group in the language of what is today called *cosets*. While Cauchy's proof implicitly used the idea of a coset, we have refrained from explicitly using that language in the interest of clarity. For an introduction to cosets based on primary sources, and the companion ideas of a *quotient group*, see the student project "Otto Hölder's Formal Christening of the Quotient Group Concept" [Barnett, 2019], based on the first paper ever written about the quotient group concept.

(a) Show that the product of two permutations is even if and only if both permutations have the same parity (i.e., both are even or both are odd).

Note: Your proof must consider all three parity cases (even/even, odd/odd, even/odd). (*Do you see why?*)

(b) Let A_n be the subset of S_n consisting of all even permutations.
Prove that A_n is a subgroup of S_n by showing that A_n is a non-empty subset of S_n that is closed under products.[25] **Note:** A_n is called the *alternating subgroup*.

(c) Explain why the set $S_n - A_n$ of all odd permutations is never a subgroup of S_n. Give at least two reasons. *Hint: Footnote 23 can help you come up with a second reason.*

(d) Show that S_n contains an equal number of even and odd permutations by letting $A_n = \{\alpha_1\,,\,\alpha_2\,,\,\ldots\,,\alpha_k\}$ and $S_n - A_n = \{\beta_1\,,\,\beta_2\,,\,\ldots\,,\beta_m\}$, where $k, m \in \mathbb{Z}^+$, and then proving $k = m$. Explain why we can then conclude that $|A_n| = \frac{n!}{2}$.
Hint: Consider the sets $\{\beta_1\alpha_1\,,\,\beta_1\alpha_2\,,\,\ldots\,,\beta_1\alpha_k\}$ and $\{\beta_1\beta_1\,,\,\beta_1\beta_2\,,\,\ldots\,,\beta_1\beta_m\}$.

3 Conclusion

Although Cauchy proved much (much!) more about the theory of permutations in his manuscripts of 1844–1845, much of it (regrettably) lies beyond the scope of this project. Subsequent work in the historical development of group theory also lies beyond our scope, including that of Cauchy's contemporary Arthur Cayley, who is credited by many with writing the first paper on the general (i.e., abstract) group concept. As we previously noted, Cauchy's work on permutation groups played a role as a particular concrete example of that more general concept in that landmark paper, [Cayley, 1854].[26] Cayley was also the first to prove a theorem, known today as Cayley's Theorem, that essentially says that *every* group, regardless of its actual elements and operation, is essentially identical to a symmetric group. In some sense, we thus see that Cauchy's work on symmetric groups identified every possible group that is out there.

Before we conclude this project, we should also comment on one final aspect related to how the symmetric group of permutations S_n is typically thought of today. Namely, rather than use a set of n letters as the underlying objects being permuted, it is standard to use permutations of the first n natural numbers: $1, 2, 3, \ldots, n$. This idea was actually first used by Cauchy himself, who employed it in an earlier paper [Cauchy, 1815a] by first introducing indexed letters (e.g., $x_1, x_2, \ldots, x_n$) to represent n variables, and then representing these variables by their subscripts alone.

Look back, for example, at the product in Task 4:

$$\begin{pmatrix} x_1\,x_2\,x_3\,x_4\,x_5 \\ x_3\,x_1\,x_2\,x_5\,x_4 \end{pmatrix}\begin{pmatrix} x_1\,x_2\,x_3\,x_4\,x_5 \\ x_5\,x_4\,x_2\,x_3\,x_1 \end{pmatrix}.$$

[25] As noted in footnote 23, showing that a non-empty subset of S_n is closed under products implies that the subset in question is also closed under inverses. In the case of a more general group, closure under inverses would instead need to be established explicitly before we could conclude that the subset in question is a subgroup of the group in question.

[26] The student project [Barnett, 2011] employs excerpts from both Cauchy and Cayley to make sense of what is today considered to be all of elementary group theory.

Using subscripts to represent each variable, Cauchy represented this product more simply as

$$\begin{pmatrix} 1\,2\,3\,4\,5 \\ 3\,1\,2\,5\,4 \end{pmatrix}\begin{pmatrix} 1\,2\,3\,4\,5 \\ 5\,4\,2\,3\,1 \end{pmatrix},$$

which can be even more simply written using cycle decomposition:

$$[(1,\,3,\,2)(4,\,5)]\,[(1,\,5)(2,\,4,\,3)]\,.$$

You can check that the final product in this example is the 5-cycle (1, 4, 2, 5, 3). The main point we wish to make here, however, is that mathematicians today think of S_n as a set of permutations on numbers (e.g., $1, 2, 3, 4, 5$), rather then a more cumbersome version of these same permutations involving letters, either indexed or not. In fact, it is something of a mystery why Cauchy did not do this in his later works on permutation theory. This may have been because he was no longer thinking of the letters as variables in functions, but rather treating permutations as interesting mathematical objects in their own right (which they are!).

As illustrations of the notation currently in use, we list the elements of the symmetric groups S_2 and S_3 in this form:

$$S_2 = \{\,(1)(2)\,,\,(1,\,2)\,\}$$

$$S_3 = \{\,(1)(2)(3)\,,\,(1,\,2,\,3)\,,\,(1,\,3,\,2)\,,\,(1,\,2)\,,\,(1,\,3)\,,\,(2,\,3)\,\}\,.$$

Note that the identity permutation is written here as the product of 1-cycles, in order to avoid any possible confusion about whether '1' is the identity permutation or one of the numbers being permuted. In part because of this potential confusion, it has also become standard practice to label the identity permutation as 'ε' (rather than '1'); thus, we might write '$(1,\,3,\,2)^3 = \varepsilon$', or '$XY = X \Rightarrow Y = \varepsilon$'. As you gain practice with permutation computations using the currently standard notation in Task 26 below, watch for ways in which the identity permutation ε can be used to simplify computations — but also be careful to avoid the trap of using commutativity where it doesn't apply!

Task 27 (a) Find the cycle decomposition of the following.

(i) $\begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 1\,3\,2\,5\,6\,4 \end{pmatrix}$ (ii) $\begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 7\,3\,5\,2\,4\,6\,1 \end{pmatrix}$ (iii) $\begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 6\,2\,5\,1\,4\,3 \end{pmatrix}^{-1}$

(b) Find each of the following products; write each as the product of disjoint cycles.

(i) $(1,\,3,\,2,\,5)(1,\,5,\,4)(2,\,3,\,6,\,4)$
(ii) $(1,\,5,\,4,\,2)^{-1}(4,\,2,\,3)(1,\,5,\,4,\,2)$
(iii) $[(1,\,2,\,5,\,4)(3,\,1,\,4)]^3$
(iv) $(1,\,2,\,5,\,4)^3(3,\,1,\,4)^3$

(c) Determine the order of each of the following permutations. Justify your answer.

(i) $(7,\,1,\,4,\,5,\,3)$
(ii) $(7,\,1,\,4,\,5,\,3)^{-1}$
(iii) $(7,\,1,\,4)(5,\,3)$
(iv) $(7,\,1,\,4)(7,\,3)$
(v) $(3,\,1,\,4)(1,\,5,\,6)$
(vi) $(3,\,1,\,4)(7,\,5,\,6)$

References

Barnett, J. H. (2011). Abstract Awakenings in Algebra: Early Group Theory in the Works of Lagrange, Cauchy, and Cayley. At `https://www.cs.nmsu.edu/historical-projects/projects.php`.

Barnett, J. H. (2017). The Roots of Early Group Theory in the Writing of Lagrange. At `https://digitalcommons.ursinus.edu/triumphs_abstract/`.

Barnett, J. H. (2019). Otto Hölder's Formal Christening of the Quotient Group Concept. At `https://digitalcommons.ursinus.edu/triumphs_abstract/`.

Cauchy, A. (1815a). Mémoire sur le nombre des valeurs qu'une fonction peut acquérir, lorsqu'on y permute de toutes les manières possibles les quantités qu'elle renferme (Memoir on the number of values that a function can acquire, when the quantities it contains are permuted in all possible ways). *Journal de l'École Polytechnique*, 17(10):1–28. Also in *Œuvres complètes de Augustin Cauchy*, Série 2, Tome 1 (1905), 64–90.

Cauchy, A. (1815b). Mémoire sur les fonctions que ne peuvent obtenir que deux valeurs égales et de signes contraires par suite des transpositions opérées entre les variables qu'elles renferment (Memoir on functions that can only obtain two equal values with opposite signs as a result of transpositions between the variables they contain). *Journal de l'École Polytechnique*, 17(10):29–117. Also in *Œuvres complètes de Augustin Cauchy*, Série 2, Tome 1 (1905), 91–169.

Cauchy, A. (1844). Mémoire sur les arrangements que l'on peut former avec des lettres données, et sur les permutations ou substitutions à l'aide desquelles on passe d'un arrangement à un autre (Memoir on the arrangements that can be formed with given letters, and on the permutations or substitutions by means of which one passes from one arrangement to another). *Exercises d'Analyse et de Mathématiques Physiques*, 3:151–242. Also in *Œuvres complètes de Augustin Cauchy*, Série 2, Tome 13 (1933), 171–282.

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

Otero, D. (2018). Determining the Determinant. At `https://digitalcommons.ursinus.edu/triumphs_linear/2`.

Roth, R. L. (2001). A History of Lagrange's Theorem on Groups. *Mathematics Magazine*, 74(2):99–108.

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

Notes to the Instructor

PSP Content: Topics and Goals

This Primary Source Project (PSP) draws on works by Augustin-Louis Cauchy to introduce aspects of the theory of finite groups within the concrete context of permutation groups. It is extracted from the second section of the extended PSP "Abstract Awakenings in Group Theory" (described in a later subsection of these Notes) in which excerpts from Cauchy's work on permutations are used to introduce students to the concept of a permutation group. As described in the introduction of this PSP, Cauchy's work on permutations grew out of efforts to find formulas for higher degree polynomial equations that linked relations between a type of function called a 'permutation' to the solution of equations by radicals. His own research, however, also marked a distinct break with the problem of solution by radicals and led him to establish a more general theory of permutations that was fully independently of the theory of equations. In other words, it was Cauchy who first gave us a complete theory of symmetric groups by studying their structure as an object of interest in its own right. Through excerpts from his writings on this theory, this project develops the elementary theory of symmetric groups as it appears in a junior-level course on abstract algebra, up to and including a proof of Lagrange's Theorem for S_n.

Student Prerequisites

Beyond a certain level of mathematical maturity, commensurate with a typical Calculus II background, there are no pre-requisites for this project. In particular, absolutely no familiarity with group theory is assumed in this PSP! Instead, the project from which is it extracted was designed to be a students' very first encounter with group-related ideas.

PSP Design and Task Commentary

This PSP begins with a short (un-numbered) historical introductory section that describes how the problem of algebraic solvability of polynomials led to the development of group theory and situates Cauchy's work on permutations within that mathematical context. It then consists of two main sections.

Section 1 focuses on the multiplication of permutations and its properties, including inverses, order, cyclic decomposition, and even/odd permutations. It is divided into four subsections (Multiplying Permutations; Permutation Order; Cycles and Transpositions; and Inverses and More), each of which constitutes about one day of in-class work. The concept of a cyclic group is introduced (without using that terminology) in Tasks 9 & 10, which should likely be discussed as a whole-group at least briefly. Task 17 develops the important concepts of even/odd permutations and should not be omitted from in-class work and discussion. Several other tasks in this section work well as individual homework; these include Task 6 and Task 12.

Section 2 then brings in the definition and elementary theory of permutation groups ('system of conjugate permutations' in Cauchy's terminology). The main focus of this section is a detailed study of Cauchy's proof of Lagrange's Theorem for groups of permutations is studied. The concrete language of that proof allows students to develop an understanding of its meaning without becoming lost in the abstraction of cosets, partitions and equivalence relations, while its complete generalizability of the proof to any finite group prepares them to make the transition to that level of abstraction later in the project/course. Modern notation for S_n and the definition of a subgroup are introduced into the project

following Cauchy's proof of Lagrange's Theorem, and Task 24 prompts students to write a complete formal proof of Lagrange's Theorem for S_n following the model of Cauchy's proof of that theorem. Task 26 also introduces the Alternating Group A_n using its modern notation.

The project concludes (Section 3) with some brief comments on the next stage of development in the history of group theory and a short exercise that employs modern permutation notation as a means to consolidate students' skill with operations on permutations.

Suggestions for Classroom Implementation

To reap the full mathematical benefits offered by this PSP, students should be required to read assigned sections in advance of any in-class discussion, or to work through reading excerpts together in small groups in class. The author's method of ensuring that advance reading takes place is to require student completion of daily "Reading Guides" based on the assigned reading for the next class meeting. 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. A typical guide includes a few "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 discussion.[27] On occasion, tasks are also assigned as follow-up to a prior class discussion. Students can also be encouraged to record any questions or comments they have about the assigned reading on their guide, or explicitly prompted to write 1–3 questions or comments about a particular primary source excerpt; responses to the latter type of prompt can be especially useful as starting points for in-class discussions and as feedback to the instructor. In order to incorporate advance preparation into course grades, reading guides are collected each class period for instructor review and scoring prior to the next class period. The author's students receive credit based only on completion (with no penalty for errors in solutions).

With regard to PSP implementation, a combination of small-group work, whole-class discussions, student presentations and homework assignments drawn from the PSP tasks is recommended in order to take advantage of the variety of questions provided in the PSP. The Sample Implementation Schedule below includes suggestions concerning instructional strategies that are especially well-suited to different parts of the PSP. For small-group work on individual tasks, the author recommends providing students with a copy of the task (with space provided to complete each part thereof). LaTeX code of the entire PSP may be requested from the author to facilitate preparation of such 'in-class task sheets' and/or advance Reading Guides.

Sample Implementation Schedule (based on a 50-minute class period)

The following 7-day sample schedule assumes completion of the entire PSP in about 2 weeks of class time. The recommended small-group discussion/work time should naturally be supplemented with whole-class discussions as deemed appropriate by the instructor.

[27] Experience has proven the value of reproducing the full text of any assigned project task on the guide itself, with blank space deliberately left below each question for students' response. This not only makes it easier for students to record their thoughts as they read, but also makes their notes more readily available to them during in-class discussions and easier for the instructor to efficiently review for completeness or a quick assessment of students' understanding.

- **Advance Preparation Work for Day 1** (to be completed before class)
  Read the (un-numbered) introduction and the introduction to Section 1 (stopping just above Subsection 1.1), and complete Task 1 for class discussion.
- **Day 1 of Class Work** Whole class and/or small group discussion of the following:
  - (Optional) Historical and mathematical ideas from the introduction, if desired.
  - Mathematical concepts in the introduction to Section 1, including answer to Task 1.
  - Complete Subsection 1.1, through Task 4.
  - Time permitting, begin reading Subsection 1.2.
- **Advance Preparation Work for Day 2** (to be completed before class)
  Read all of Subsection 1.2, and complete Tasks 5 & 7 (skipping Task 6) for class discussion.
- **Day 2 of Class Work** Whole class and/or small group discussion of the following:
  - Mathematical concepts in assigned Section 1.2 reading, including answers to Tasks 5 & 7.
  - Begin Subsection 1.3, aiming for completion of Task 11.
- **Advance Preparation Work for Day 3** (to be completed before class)
  Complete Tasks 8–11 in Subsection 1.3 as needed. (Skip Task 12.) Begin reading Subsection 1.4 (through Task 15), and complete Tasks 14–15 for class discussion.
- **Day 3 of Class Work** Whole class and/or small group discussion of the following:
  - Mathematical concepts in assigned reading from Section 1.4, including answers to Tasks 14–15.
  - Skipping Task 16, complete as much of Task 17 as time permits.

- **Final Homework Assignment for Section 1** – following completion of all in-class work for Section 1, a complete formal write-up of Tasks 6, 12, 13, 14, 15, 16, 17 should be assigned.

- **Advance Preparation Work for Day 4** (to be completed before class)
  Begin reading Section 2 (through Task 18), and complete Task 18 for class discussion.
- **Day 4 of Class Work** Whole class and/or small group discussion of the following:
  - Mathematical concepts in assigned reading from Section 2, including answers to Task 18.
  - Continue Section 2, working at least through Task 20.
- **Advance Preparation Work for Day 5** (to be completed before class)
  Continue reading Section 2 (through Task 21), and complete Task 21 for class discussion.
- **Day 5 of Class Work** Whole class and/or small group discussion of the following:
  - Mathematical concepts in assigned reading from Section 2, including answers to Task 21.
  - Continue Section 2, ending with Task 26.

– A whole-class discussion to set up the reading of the Cauchy's proof of Lagrange's Theorem could also be useful towards the end of this class session.

- **Advance Preparation Work for Day 6** (to be completed before class)
  Continue reading Section 2 (through Task 23), and begin work on Task 23 for class discussion.
- **Day 6 of Class Work** Whole class and/or small group discussion of the following:
  – Complete Task 23.
  – Time permitting, read or discuss the secondary commentary between Tasks 23 and 24.
- **Advance Preparation Work for Day 7** (to be completed before class)
  Read the remainder of Section 2 and all of Section 3, but with no assigned tasks.
- **Day 7 of Class Work** Whole class and/or small group discussion of the following:
  – Mathematical concepts in assigned reading from Section 2, including any remaining questions about Task 23; **note that only part of this day may be needed to wrap up class work on the PSP!**
- **Final Homework Assignment** – following completion of all in-class work, a complete formal write-up of Tasks 23, 24, 25, 26 should be assigned.

Connections to other Primary Source Projects (PSPs)

The PSP "Determining the Determinant" [Otero, 2018] listed in the References also focuses on Cauchy's work on permutations, but as a means to introduce students to the important linear algebra concept of a determinant.

Abstract algebra instructors who wish to offer a more intensive primary source based exploration of that discipline will want to consider the following additional PSPs which address core topics from the standard curriculum of a junior-level abstract algebra course. Each has been successfully site tested at several institutions as a replacement for a textbook, either for a portion or the entirety of the course. Further information about structuring an entire Abstract Algebra course around PSPs in this collection is available from the author of these projects.

- "Abstract Awakenings in Group Theory: Early group theory in the works of Lagrange, Cauchy, and Cayley"[28]

  The centerpiece of this extended PSP is the 1854 inaugural paper on abstract groups, 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 the project begins with the material from Lagrange

[28]To obtain the most recent version of "Abstract Awakenings in Group Theory", contact its author at at `janet.barnett@csupueblo.edu`, or visit `www.cs.nmsu.edu/historical-projects/projects.php` for an earlier version.

in the PSP "The Roots of Early Group Theory in the Works of Lagrange" (described below). Section 2 then employs selections from writings by Cauchy in the PSP "An Independent Theory of Permutations: Early Group Theory in the Work of A.-L. Cauchy" (also described below). The Abstract "Awakenings" 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.

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. 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, including: 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 that also states the definitions of normal subgroup and factor group; this material is, however, more fully and effectively developed in the current PSP.

- "The Roots of Early Group Theory in the Works of Lagrange"[29]

  This PSP draws on works by one of the early precursors of abstract group, French mathematician J. L. Lagrange. 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.

  The design of this project is based on the first section of the extended PSP "Abstract Awakenings in Group Theory" described above. 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 easily shift over to the PSP "Abstract Awakenings of Algebra". 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 in much, if any, detail.

[29]To obtain the most recent version of "The Roots of Early Group Theory in the Works of Lagrange", visit `https://blogs.ursinus.edu/triumphs/`. An alternative version of this PSP that adopts a more open-ended/inquiry-based approach in which all resolvent equation examples are presented as tasks for students to complete themselves is also available upon request from its author at `janet.barnett@csupueblo.edu`.

- "Otto Hölder's Formal Christening of the Quotient Group Concept"[30]

  This PSP draws on excerpts from the paper by Otto Hölder in which he gave what is now considered to be the first "modern" definition of quotient groups. Although quotient groups implicitly appeared in Galois' work on algebraic solvability in the 1830s, that work itself pre-dated the development of an abstract group concept. Even Cayley's 1854 paper in which a definition of an abstract group first appeared was premature, and went essentially ignored by mathematicians for decades. Permutation groups were extensively studied during that time, however, with implicit uses of quotient groups naturally arising within it. Jordan, for example, used the idea of congruence of group elements modulo a subgroup to produce a quotient group structure. Thus, when Hölder wrote his paper in 1889, he was able to treat the concept as neither new nor difficult. This PSP, designed for a first course in abstract algebra, draws on excerpts from that paper as a means to introduce students to the concepts of a normal subgroup, a quotient group, the Fundamental Homomorphism Theorem and related elementary results. Excerpts from earlier works by Cauchy, Cayley and Jordan in which precursors of these ideas appeared are also treated in three optional and independent appendices.

  No prior familiarity with normal subgroups, quotient groups, or group homomorphisms is assumed in this project. To the contrary, the project is designed to serve as students' first introduction to these three concepts and their related theory, following their study of more elementary group theory. It is assumed that students are comfortable with the definitions and examples of groups and subgroups, along with related proof techniques (e.g., for establishing closure under products) and basic results (e.g., Lagrange's Theorem for finite groups). Although the concept of a coset also naturally makes an appearance in this project, the definition given in the project could serve as students' first introduction to this concept. In particular, it not necessary for students to have seen a proof of Lagrange's Theorem via cosets and equivalence classes; an alternate proof of this theorem that uses neither of these notions is included in Appendix I of the project. In addition to being fully self-contained with respect to the study of group homomorphisms, the project's treatment of the Fundamental Homomorphism Theorem also requires no prior study of group isomorphisms. It is, however, standard (and helpful!) for students enrolled in an abstract algebra course to have previously met the idea of an isomorphism in a linear algebra course.

- "Richard Dedekind and the Creation of an Ideal: Early Developments in Ring Theory"[31]

  This PSP draws on the 1877 version of Dedekind's theory of ideals as a means to introduce students to the elementary theory of rings and ideals. Characteristics of Dedekind's work that make it an excellent vehicle for students in a first course on abstract algebra include his emphasis on abstraction, his continual quest for generality and his careful methodology. The 1877 version of his ideal theory (the third of four versions he developed in all) is an especially good choice for students to read, due to the care that Dedekind devoted therein (via examples from number theory that are readily accessible to students) to motivating why ideals are of interest to mathematicians. In this regard, unique prime factorization (and the failure thereof in certain integral domains) plays a central role.

[30] To obtain the most recent version of 'Otto Hölder's Formal Christening of the Quotient Group Concept", visit `https://blogs.ursinus.edu/triumphs/`

[31] To obtain the most recent version of "Richard Dedekind and the Creation of an Ideal: Early Developments in Ring Theory", visit `https://blogs.ursinus.edu/triumphs/`.

Other specific topics developed in the PSP include the following: rings, integral domains, fields, zero divisors, ideals, principal ideals, prime ideals, and maximal ideals.

No prior familiarity with ring theory is assumed. The project has also been successfully used with students who had not yet studied group theory. For those who have not yet studied group theory (or those who have forgotten it!), basic definitions and results about identities, inverses and subgroups are fully stated when they are first used within the PSP (with the minor exception of Lagrange's Theorem for Finite Groups which is needed for one part of one task).

Recommendations for Further Reading

Instructors who wish to take a deeper dive into the present PSP's context or content during its classroom implementation will find the book *The Genesis of the Abstract Group Concept:A Contribution to the History of the Origins of Abstract Group Theory*, [Wussing, 1984], to be of particular interest.

Acknowledgments

The development of this student project has been partially supported by the Learning Discrete Mathematics and Computer Science via Primary Historical Sources (LDM) project, with funding from the National Science Foundation's Course, Curriculum & Laboratory Improvement (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 represent the views of the National Science Foundation.

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

For more information about Transforming Instruction in Undergraduate Mathematics via Primary Historical Sources (TRIUMPHS), visit `https://blogs.ursinus.edu/triumphs/`.