

# Otto Hölder's Formal Christening of the Quotient Group Concept

Janet Heine Barnett\*

April 19, 2019

In 1854, British mathematician Arthur Cayley (1821–1895) published the paper *On the theory of groups, as depending on the symbolic equation  $\theta^n = 1$*  [Cayley, 1854]. Although it is recognized today as the inaugural paper in abstract group theory, Cayley's ground-breaking paper went essentially ignored by mathematicians for decades; the mathematical world, it seems, was not quite ready for the study of such abstract groups. Permutation groups, on the other hand, continued to be extensively studied. As a natural by-product of their work on certain problems related to permutation groups, a number of mathematicians also began to make implicit use of a more abstract type of algebraic structure, referred to today as a 'quotient group.' When the German mathematician Otto Hölder (1859–1937) gave the first explicit definition of a quotient group in 1889, he thus treated the concept as neither new nor difficult. As a result of this and other related developments in the study of algebra, abstract group theory in general, and quotient groups in particular, came to play a central role in a number of mathematical sub-disciplines by the end of the nineteenth century, as they continue to do today. In this project, we will study the concept of a quotient group as it was developed by Hölder in his article [Hölder, 1889], entitled "Zurückführung einer beliebigen algebraischen Gleichung auf eine Kette von Gleichungen (Reduction of an arbitrary algebraic equation to a chain of equations)."

Hölder began his mathematical studies at the University of Berlin, but completed his doctorate on the use of arithmetic means to study analytic functions and summation at the Eberhard-Karls University of Tübingen in 1882. He then hoped to complete the additional post-doctoral qualification (called the *Habilitation*) that was required to lecture at a German university. He eventually did so at the University of Göttingen, after being denied the opportunity to habilitate at Leipzig. He was first required to submit a second doctoral dissertation to Göttingen when that university declined to accept his Tübingen doctorate; this second dissertation was also in analysis, on the topic of Fourier series convergence. While at Göttingen, however, Hölder's interests in group theory were encouraged through his interactions with various faculty there who were working in algebra; his initial interest in algebra was probably due to the influence of Leopold Kronecker (1823–1891), with whom Hölder studied in Berlin. Following a brief period of mental collapse, Hölder returned to the University of Tübingen as a professor in 1890. He later moved to the University of Leipzig

---

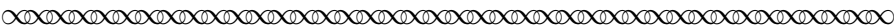
\*Department of Mathematics and Physics, Colorado State University-Pueblo, Pueblo, CO 81001-4901; [janet.barnett@csupueblo.edu](mailto:janet.barnett@csupueblo.edu).

where he held both professorial and administrative positions. It was during his years in Tübingen and Leipzig that Hölder made numerous contributions to group theory: he was the first to formally study quotient groups as an abstract concept, made important advancements in the search for simple groups, and introduced the concepts of inner and outer group automorphisms. Although Hölder’s interests shifted to the geometrical study of the projective line and to certain philosophical questions in his later years, it is his work in group theory that is best remembered today. Foremost among this work is the theorem on the uniqueness of the factor groups in a composition series, known today as the Jordan-Hölder theorem, which Hölder proved in its most general form in the 1889 *Mathematische Annalen* paper which forms the basis of this project.

We begin in Section 1 with a look at Hölder’s definition of a group, which we compare briefly to today’s current definition. In Section 2, we consider his discussion of a certain special type of subgroup that is related to both the concept of a quotient group and to a type of function known as a homomorphism, two concepts that in turn have a special connection to each other. Section 3 briefly brings in Hölder’s original motivation for providing a definition of the quotient group concept, with a brief discussion of an early (and more concrete) version of the theorem known today as the Jordan-Hölder Theorem. The concept of a quotient group is examined in detail in Sections 4 and 5 of this project. The closing Section 6 begins by looking at the concept of a homomorphism independently of quotient groups, before bringing quotient groups and homomorphisms together in Hölder’s statement of the Fundamental Homomorphism Theorem.

# 1 Hölder’s Definition of a Group

Let’s begin by reading Hölder’s definition of a group from his 1889 paper, and compare it to what has since become the standard definition for this basic algebraic structure.<sup>1</sup>



## I. Group theoretic section<sup>2</sup>

### § 1. Defining properties of groups

The theorems developed in this section are valid for any group which consists of a *finite* number of elements.<sup>3</sup> The nature of the elements is immaterial. Only the properties of a group will be assumed, which can be encapsulated in the following definitions:\*

---

<sup>1</sup>To set them apart from the project narrative, all original source excerpts are set in sans serif font and bracketed by the following symbol at their beginning and end: ∞∞∞∞∞∞∞

<sup>2</sup>The translation of the excerpts from Hölder’s paper that are used in the project is due to George W. Heine III and David Pengelley, 2017.

<sup>3</sup>Hölder himself used the word ‘operation’ here. Since his treatment of groups is fully general, and in keeping with today’s treatment of the subject, we have replaced the word ‘operation’ by the word ‘element’ throughout.

\*Hölder’s footnote: Regarding the definition of group compare also Dyck, Grouptheoretic studies, *Math. Ann.* vol. XX.

- 1) Each pair of elements, composed (multiplied) in a determined sequence, should yield a uniquely determined element, which likewise belongs to the same aggregate.
- 2) In each composition of elements, the associative law holds, while the commutative law need not.
- 3) From each of the two symbolic equations containing the elements  $A, B, C$ ,

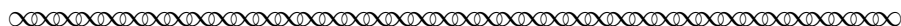
$$AB = AC, \quad BA = CA$$

it can be concluded that

$$B = C.$$

A consequence of this determination, in the context of a finite number of elements, is that a so-called *identity* element  $J$  exists, actually a single one, which leaves all others unchanged by multiplication, and that for each element  $A$ , a unique determined inverse element  $A^{-1}$  exists, so that

$$A A^{-1} = A^{-1} A = J.$$



### Task 1

Compare the definition of a group given by Hölder to the definition typically found in today's textbooks. How are these definitions the same? How are they different?

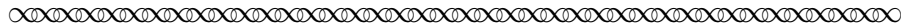
### Task 2

Notice that Hölder claimed in this excerpt that, for a *finite* group  $G$ , the three conditions that he stated in the previous excerpt suffice to prove that  $G$  contains an identity element  $J$ , as well as inverses for each element of  $G$ .

- (a) Prove that Hölder's claim concerning the identity element  $J$  is correct.  
State clearly where the assumption that  $G$  is finite is used.
- (b) Now assume that  $G$  is a finite set together with a binary operation that satisfies just Hölder's conditions 1 and 2. Also assume that  $G$  contains an identity element  $J$ . Prove that every element  $A$  in  $G$  has an inverse element  $A^{-1}$  in  $G$ . Again, state clearly where the assumption that  $G$  is finite is used.
- (c) Is it possible for either of the theorems from part (a) and part (b) to fail when  $G$  is infinite? Explain why or why not.

## 2 A Special Type of Subgroup

In the second section of his paper, Hölder described a special type of subgroup that is needed for the construction of a quotient group. Today, this type of subgroup is called a ‘normal subgroup.’ We will use Hölder’s term ‘distinguished subgroup’ for this type of subgroup in the excerpts that we take from his paper, but use the two terms interchangeably elsewhere in this project. Recall first that a subgroup  $H$  of a group  $G$  is a non-empty subset of  $G$  that is itself a group, which requires  $H$  to be closed under products and inverses. (Notice that Hölder himself stated no definition of subgroup, but simply assumed that his readers are already familiar with the concept.)



### § 2. Distinguished subgroups

If the elements

$$B, B_1, B_2, \dots$$

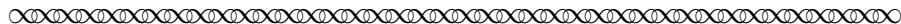
form a “subgroup” of the entire group, then the elements “transformed with the help of the element  $A$ ”,

$$A^{-1}BA, A^{-1}B_1A, A^{-1}B_2A, \dots,$$

also form a group, which itself will be called *transformed* from the first subgroup.

A subgroup which is identical with all of its transforms is called, after an expression of Mr. Klein, *distinguished*, or after Mr. König (Math. Annalen vol. 21) an *invariant* subgroup. In the older parlance, such a subgroup was said to be “commutable with all the elements of the entire group.” That is, if  $A$  denotes an arbitrary element of the whole group, and  $B$  an element of the subgroup, then the products  $AB$  and  $BA$  are respectively representable in the forms  $B'A$  and  $AB''$ , where  $B'$  and  $B''$  denote appropriately chosen elements of the subgroup.

A distinguished subgroup is called a *maximal distinguished subgroup* if there is no more extensive distinguished subgroup of the whole group containing it.



Letting  $G$  be a group,  $H$  a subgroup of  $G$  and  $a \in G$ , we can define and denote what Hölder called a ‘transform of the subgroup  $H$ ’ as follows:

$$a^{-1}Ha = \{a^{-1}ha \mid h \in H\}.$$

**Task 3** Prove that  $a^{-1}Ha$  is indeed a subgroup of  $G$ .

**Task 4**

Consider the specific group<sup>4</sup>  $G = S_3$ , and denote the identity permutation by  $e$ .

- (a) Let<sup>5</sup>  $H = \langle (1, 2, 3) \rangle = \{e, (1, 2, 3), (1, 3, 2)\}$ .

Find the transformed subgroup  $a^{-1}Ha$  for every element  $a \in S_3$ .

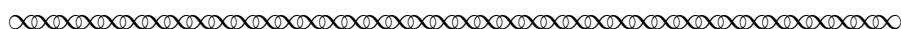
What do you notice about the transformed subgroups in this case?

- (b) Now let  $K = \langle (2, 3) \rangle = \{e, (2, 3)\}$ .

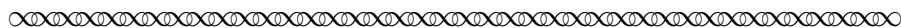
Find the transformed subgroup  $a^{-1}Ka$  for every element  $a \in S_3$ .

What do you notice about the transformed subgroups in this case?

You may have noticed that one of the two examples in Task 4 has the special property which Hölder described as follows:



A subgroup which is identical with all of its transforms is called, after an expression of Mr. Klein, *distinguished*, or after Mr. König (Math. Annalen vol. 21) an *invariant* subgroup. In the older parlance, such a subgroup was said to be “commutable with all the elements of the entire group.” That is, if  $A$  denotes an arbitrary element of the whole group, and  $B$  an element of the subgroup, then the products  $AB$  and  $BA$  are respectively representable in the forms  $B'A$  and  $AB''$ , where  $B'$  and  $B''$  denote appropriately chosen elements of the subgroup.



In Definition 1, Hölder’s definition of a ‘distinguished subgroup’ is stated using the notation introduced in Task 3 above. As noted earlier, we will also refer to such subgroups using the current terminology of a ‘normal subgroup.’

### Definition 1

Let  $G$  be a group and  $H$  a subgroup of  $G$ .

$H$  is a *normal* (or *distinguished*) *subgroup* of  $G$  if and only if  $(\forall a \in G)(a^{-1}Ha = H)$ .

When  $H$  is a normal subgroup of  $G$ , we write  $H \triangleleft G$ .

Notice Hölder’s remark that the set equality ‘ $a^{-1}Ha = H$ ’ does NOT mean that an individual element  $a^{-1}ha$  from  $a^{-1}Ha$  will be equal to the element  $h$ . In other words, we can NOT assume that  $a^{-1}ha = h$  when  $a \in G$  and  $h \in H$  for a normal subgroup  $H$ . Of course, if  $G$  is abelian, then  $a^{-1}ha = h$  for all  $a \in G$  and  $h \in H$  — but not all groups are abelian! Indeed, you will

<sup>4</sup>Recall that for  $n \in \mathbb{Z}^+$ , the notation  $S_n$  denotes the symmetric group on  $n$  variables.

<sup>5</sup>Given any group  $G$  and an element  $a \in G$ , we denote the subgroup generated by  $a$  as  $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ .

have found in Task 4(a) above that  $(1, 2)^{-1}H(1, 2) = H$ , even though it is quite clear, for instance, that  $(1, 2)^{-1}(1, 2, 3)(1, 2) \neq (1, 2, 3)$ . Instead, we see that  $(1, 2)^{-1}(1, 2, 3)(1, 2) = (1, 3, 2)$  — which is fine, since  $(1, 3, 2) \in H$ . Or, using the fact that  $(1, 2)^{-1} = (1, 2)$  to rewrite this last equality as  $(1, 2)(1, 2, 3) = (1, 3, 2)(1, 2)$  and setting  $a = (1, 2)$ ,  $h = (1, 2, 3)$  and  $h' = (1, 3, 2)$ , we see that  $ah = h'a$  where both  $h$  and  $h'$  are elements of  $H$ . Adapting Hölder's comments in the previous excerpt to the lower case letters that we have introduced here, the set equality ' $a^{-1}Ha = H$ ' thus only implies that:

“the products  $ah$  and  $ha$  are respectively representable in the forms  $h'a$  and  $ah''$ , where  $h'$  and  $h''$  denote appropriately chosen elements of the subgroup.”

According to Hölder, this idea was described in ‘the older parlance’ by the expression ‘**the subgroup is commutable with all the elements of the entire group.**’ This gives us the following alternative definition for a normal subgroup which is often used today:

**Definition 1'**

Let  $G$  be a group and  $H$  a subgroup of  $G$ .

$H$  is a *normal (or distinguished) subgroup* of  $G$  if and only if  $(\forall a \in G)(aH = Ha)$ , where  $aH = \{ah \mid h \in H\}$  and  $Ha = \{ha \mid h \in H\}$  respectively.

Recalling that the sets  $aH$  and  $Ha$  are called *cosets of  $H$* , this definition says that  $H$  is normal if and only if the left and right cosets corresponding to each element are equal. We will meet cosets again when we pick up our reading of Hölder in the next section. The tasks in the rest of this section first provide some practice with using Definition 1' and two other methods that can be used to prove a particular subgroup is normal.

**Task 5** Let  $G$  be a group, and recall that the center of  $G$  is the subgroup defined by

$$C = \{x \in G \mid (\forall y \in G)(yx = xy)\}.$$

Use Definition 1' to prove that  $C$  is a normal subgroup in  $G$

(You can assume  $C$  is a subgroup of  $G$ , and just prove the normality of  $C$  in  $G$ .)

**Task 6** This task introduces another property that could be used to define a normal subgroup.

Let  $G$  be a group and  $H$  a subgroup of  $G$ .

We say that  $H$  is *closed under conjugates* if and only if  $(\forall a \in G)(\forall h \in H)(a^{-1}ha \in H)$ .

Prove that  $H \triangleleft G$  if and only if  $H$  is closed under conjugates.

(An element of the form  $a^{-1}ha$  is called a *conjugate* of  $h$ .)

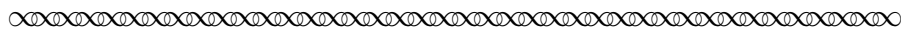
**Task 7** Given a group  $G$ , a *commutator* of  $G$  is any element of the form  $xyx^{-1}y^{-1}$ , where  $x, y \in G$ .

Suppose  $H$  is a subgroup of  $G$  such that  $H$  contains all the commutators of  $G$ .

Show that  $H$  is a normal subgroup of  $G$  by proving that  $H$  is closed under conjugates.

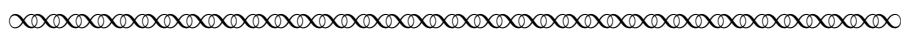
**Task 8**

In this task, we look at an excerpt from a paper by Eugen Netto<sup>6</sup> (1846–1919) that provides us another way to prove that a subgroup is normal. We begin by reading Netto's statement and proof of the theorem in question [Netto, 1882, p.81].



§71 *If a group  $G$  of order  $2r$  contains a subgroup  $H$  of order  $r$ , then  $H$  is a normal<sup>7</sup> subgroup of  $G$ .*

For if the elements<sup>8</sup> of  $H$  are denoted by  $1, s_2, s_3, \dots, s_r$ , and if  $t$  is any element of  $G$  which is not contained in  $H$ , then  $t, ts_2, ts_3, \dots, ts_r$  are the remaining  $r$  elements of  $G$ . But in the same way,  $t, s_2t, s_3t, \dots, s_rt$  are also these remaining elements. Consequently every element  $s_\alpha t$  is equal to some  $ts_\beta$ , that is, we have in every case  $t^{-1}s_\beta t = s_\alpha$  and therefore  $G^{-1}HG = H$ .



- Explain why Netto could assert that  $t, ts_2, ts_3, \dots, ts_r$  are ‘the remaining  $r$  elements of  $G$ ’ in his proof. Begin by clearly stating the assumptions that led him to this assertion.
- In the final sentence of his proof, Netto concluded that  $G^{-1}HG = H$ . State a formal definition for this equality, based on Netto's argument leading up to this conclusion:

**Definition 2**

Let  $G$  be a group and  $H$  a subgroup of  $G$ .

Then  $G^{-1}HG = H$  if and only if \_\_\_\_\_.

Why do you think that Netto himself used the phrase ‘self-conjugate subgroup’ to refer to subgroups that satisfy this equality? (See footnote 6.)

- Explain why the equation  $G^{-1}HG = H$  holds if and only if  $H$  is normal in  $G$ .
- Use Netto's Theorem to explain why<sup>9</sup>  $A_n \triangleleft S_n$  for all  $n \in \mathbb{Z}^+$ .

---

<sup>6</sup>The German mathematician Eugen Netto studied mathematics from 1866–1870 at the University of Berlin, where he attended lectures by Leopold Kronecker (1823–1891), Karl Weierstrass (1815–1897) and Ernst Eduard Kummer (1810–1893), among others. His doctoral dissertation, completed under the direction of Weierstrass and Kummer, was officially awarded in 1871. Netto then taught at a gymnasium (or secondary school) in Berlin before securing a professorship at the University of Strasbourg in 1879. He left Strasbourg in 1888 for an appointment at the University of Giessen, where he remained until the debilitating effects of Parkinson's disease forced his retirement. Although Netto worked in other areas of mathematics during his early career, he is best remembered for his contributions to group theory. His book [Netto, 1882], from which the excerpt in Task 8 is taken, was especially important for the ways in which it combined results from permutation groups with results about groups that had been developed within number theory, independently of the study of permutation groups.

<sup>7</sup>Netto himself used the expression ‘self-conjugate’ in place of the adjective ‘normal’ here; the former was another standard way of describing normality in the nineteenth century work on permutation groups.

<sup>8</sup>Netto used the term ‘substitution’ here, as was common within the context of permutation groups at the time. Since his proof is fully generalizable to any arbitrary group, we have replaced the word ‘substitution’ by the word ‘element’ in keeping with the more general context of this project.

<sup>9</sup>Recall that for  $n \in \mathbb{Z}^+$ , the notation  $A_n$  denotes the alternating subgroup which consists of all even permutations in the symmetric group  $S_n$ .

### 3 From “Factors of Composition” to “Quotient Groups”

Recall the following definition stated by Hölder at the very end of the excerpt in Section 2:

A distinguished subgroup is called a *maximal distinguished subgroup* if there is no more extensive distinguished subgroup of the whole group containing it.

## Task 9

- (a) Use set notation to complete the following re-statement of this definition:

Let  $G$  be a group with  $H \triangleleft G$ .

$H$  is a *maximal* normal subgroup of  $G$  provided the following condition holds:

If  $K \triangleleft G$  with  $H \subseteq K \subset G$ , then \_\_\_\_\_.

- (b) Let<sup>10</sup>  $G = \mathbb{Z}_{12}$  and  $H = \langle 2 \rangle$ . Since  $G$  is abelian, we know that  $H$  is normal in  $G$ .  
*(In fact, every subgroup of  $G$  is normal in  $G$  — make sure you see why this is true!)*  
 Show that  $H$  is a maximal normal subgroup of  $G$ .

- (c) Again let  $G = \mathbb{Z}_{12}$ .  
Find a second maximal normal subgroup  $K$  of  $G$ , different from the one in part (b).  
Explain how you know that your example  $K$  is maximal.

Hölder began Section 3 of his paper by stating the following intriguing property related to series (or chains) of maximal normal subgroups.

### § 3. The factors of composition

Of special importance is a series introduced by Mr. C. Jordan. Namely, if  $G$  is any group, then a series of groups

$$G, G', G'', \dots J$$

is built, such that each group of this sequence is a maximal distinguished subgroup of the previous one, and the last group, denoted  $J$ , contains only the identity element. Such a series is called a *series of composition*. Now if the groups of the series contain

$$n, n', n'', \dots 1$$

elements respectively, then

$$\frac{n}{n'}, \frac{n'}{n''}, \dots$$

are the numbers which Mr. C. Jordan introduced into the theory as *factors of composition*. These factors are completely determined, except for their succession, despite the possibility of altering the series of composition.<sup>†</sup>

But this theory of the factors of composition must then be deepened, so that the factors are interpreted as *groups*.

<sup>10</sup>Given  $n \in \mathbb{Z}^+$ , the notation  $\mathbb{Z}_n$  denotes the set of integers mod  $n$ , which forms a group under addition mod  $n$ .

<sup>†</sup>Hölder's footnote: Cf. Jordan, *Traité des substitutions*, etc., p. 42



The fact that the factors of composition are *invariant* in the way described above was well-known in Hölder’s time. Its existence (and usefulness) was discovered in connection with the problem of determining whether a given polynomial is algebraically solvable.<sup>11</sup> We omit these details, in part because they go beyond the scope of this project — but also because the alternative approach of looking instead at *quotient groups* suggested at the end of this excerpt is indeed a much deeper theory. Before we turn to this theory, let’s pause for a quick illustration of the invariance of the factors of composition.

**Task 10** Let  $G = \mathbb{Z}_{12}$ . Recall again that every subgroup of  $G$  is normal, since  $G$  is abelian.

- (a) We know (from Task 9) that  $\langle 2 \rangle$  is a maximal normal subgroup of  $G$ . By a similar proof, each of the subgroups in the following series is a maximal normal subgroup of its predecessor. (*Make sure you believe this!*)

$$\mathbb{Z}_{12} \triangleright \langle 2 \rangle \triangleright \langle 4 \rangle \triangleright \langle 0 \rangle$$

Explain why the factors of composition for this series are 2, 2, 3.

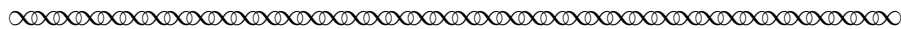
- (b) Now consider the following series of maximal normal subgroups in  $G$ :

$$\mathbb{Z}_{12} \triangleright \langle 3 \rangle \triangleright \langle 6 \rangle \triangleright \langle 0 \rangle$$

Determine the factors of composition for this chain, and compare them to those for the series in part (a). Explain how this relates to the property that Hölder described in the preceding excerpt.

## 4 Quotient Groups and Normal Subgroups

Hölder preceded his definition of the quotient group itself with the following description of what he intended to do, and a reminder to his readers about some useful background ideas.



It will be shown in the next sections that through the relationship of a group to a distinguished subgroup contained in it, a new group of generally different elements is always defined. This latter group is fully determined from an abstract standpoint, in which the substance of the elements is disregarded, and only their mutual combination considered, and for which therefore also groups obtainable uniquely from one another (*isomorphic*<sup>12</sup>) are interpreted as identical. Here’s an example.<sup>‡</sup>

<sup>11</sup>A polynomial is said to be algebraically solvable provided its roots can be obtained from its coefficients using only elementary arithmetic operations (+, −, ×, ÷) and extraction of roots. The quadratic formula, for instance, proves that every second degree polynomial is algebraically solvable. Although Niels Abel (1802–1829) and Évariste Galois (1811–1832) proved that the general polynomial of degree 5 or higher is not algebraically solvable, specific polynomials of these higher degrees may be algebraically solvable. This is the case, for instance, with the equations  $x^n - 1 = 0$ , which give us the  $n^{\text{th}}$  roots of unity.

<sup>12</sup>Hölder himself used the phrase *holohedrally isomorphic* here, while other algebraists of his time used the phrase *simply isomorphic*, to describe this notion of two “different groups” being the same from an abstract point of view. In this project, we use the current term *isomorphic*, which is formally defined today in terms of an operation-preserving bijection between the two groups. We will examine this definition more formally in Section 6.

<sup>‡</sup>Hölder’s footnote: Cf. the work of Herr Dyck in Math. Ann. vol. XX.

## § 4. The quotient defined by a group and one of its distinguished subgroups

If the symbols

$$B, B_1, B_2, \dots$$

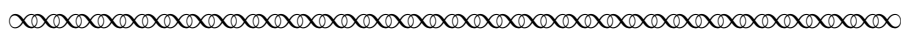
denote the elements of any subgroup  $H$ , then all the elements of the entire group  $G$  can be represented in the scheme

$$\begin{array}{cccc} B, & B_1, & B_2, & \dots \\ S_1 B, & S_1 B_1, & S_1 B_2, & \dots \\ S_2 B, & S_2 B_1, & S_2 B_2, & \dots \\ \dots & \dots & \dots & \dots \\ S_{n-1} B, & S_{n-1} B_1, & S_{n-1} B_2, & \dots \end{array}$$

where the elements

$$S_1, S_2, \dots, S_{n-1}$$

are appropriately chosen from the entire aggregate. This scheme is found already in Cauchy. Here's an example.<sup>§</sup> The same serves also for the proof that the number  $m$  of elements  $B$ , that is, the order of the subgroup, is always a divisor of the total number of elements, that is, of the order of the whole group.



### Task 11

In the preceding excerpt, Hölder noted the requirement that ‘the elements  $S_1, S_2, \dots, S_{n-1}$  are appropriately chosen from the entire aggregate’ in the construction of the scheme (or array) found in Cauchy.<sup>13</sup>

Describe how these elements must be chosen so as to ensure that every element of the group  $G$  appears in this array exactly once.

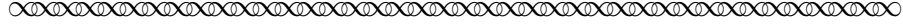
### Task 12

Hölder commented that this array also serves to prove a certain result relating the order of a finite group to the order of a subgroup. What is this theorem called today? Give a complete modern statement of it.

With these preliminaries in place, Hölder was ready to give the following definition of the quotient group. (Recall that  $B, B_1, B_2, \dots$  denote the elements of the subgroup  $H$ , while  $S_\nu, S_\mu, S_x$  denote elements of the group  $G$  in this continuation of the preceding excerpt.)

<sup>§</sup>Hölder's footnote: Cauchy: *Exercices d'analyse et de physique mathématique*, vol. III, p. 184.

<sup>13</sup>See Appendix I of this project for an excerpt from the paper in which Cauchy first constructed this array in his proof of an early version of the theorem which is now known as “Lagrange’s Theorem” in finite group theory, and some related exercises.



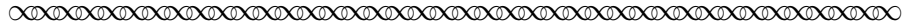
Now if the subgroup is distinguished (normal), then the theorem holds, that two arbitrary elements from two specific horizontal rows of the given schema, composed in a certain succession, must give an element of a completely determined horizontal row. Indeed, if  $\mu, \nu, \rho, \sigma$  signify four arbitrary indices, then it is always the case that<sup>14</sup>

$$\begin{aligned} S_\nu B_\rho S_\mu B_\sigma &= S_\nu S_\mu B_{\rho'} B_\sigma \\ &= S_x B_\tau \end{aligned}$$

where the index  $x$  depends only on  $\mu$  and  $\nu$ .

Thereby a composition of horizontal rows is defined. Thus one obtains new elements, which likewise form a group. This completely determined group is that which should be introduced for consideration. One could call it the *quotient* of the groups  $G$  and  $H$ , and in what follows it shall be denoted

$$G/H.$$



### Task 13

- (a) In his definition of the quotient group in the final paragraph of this excerpt, what types of objects does Hölder say are being multiplied (or ‘composed’) to obtain another object of the same kind? How many such objects are there? That is, what is  $|G/H|$ ?
- (b) According to Hölder,  $H$  must be normal in order for the following computation to go through:

$$\begin{aligned} S_\nu B_\rho S_\mu B_\sigma &= S_\nu S_\mu B_{\rho'} B_\sigma \\ &= S_x B_\tau. \end{aligned}$$

- (i) Where exactly is the assumption of normality being used?  
(Recall again that  $B, B_1, B_2, \dots$  denote the elements of the subgroup  $H$ , while  $S_\nu, S_\mu, S_x$  denote elements of the group  $G$ .)
- (ii) Why was it important for Hölder to select *arbitrary* indices  $\mu, \nu, \rho, \sigma$  for this computation?
- (iii) What did Hölder mean by the phrase ‘the index  $x$  depends only on  $\mu$  and  $\nu$ ’?

---

<sup>14</sup>A typographical error in this next equation in Hölder’s original article has been corrected throughout this project.

How interesting! Hölder has just described how we can take two *horizontal rows* in an array, and multiply them to obtain another ‘completely determined’ *horizontal row* of this same array! In other words, the elements of the quotient group  $G/H$  are actually *subsets* of the group  $G$ . Notice that these subsets (or horizontal rows) are the cosets  $S_1H, S_2H, \dots$  of the normal subgroup  $H$  for certain appropriately chosen elements  $S_1, S_2, \dots, S_{n-1}$  of  $G$ . This is easy to see from the array itself, which we re-write here using the current convention of representing elements of  $G$  by lower case letters:

$$\begin{array}{rcll} H & = & \{b, & b_1, & b_2, & \dots \} \\ s_1H & = & \{s_1b, & s_1b_1, & s_1b_2, & \dots \} \\ s_2H & = & \{s_2b, & s_2b_1, & s_2b_2, & \dots \} \\ \vdots & & \vdots & \vdots & \vdots & \\ s_kH & = & \{s_kb, & s_kb_1, & s_kb_2, & \dots \} \\ \vdots & & \vdots & \vdots & \vdots & \end{array}$$

Further simplifying the notation by dropping the subscripts, we can thus define the set  $G/H$  more simply as:

$$G/H = \{sH \mid s \in G\}.$$

It is important to remark here that it’s quite possible for two different elements of  $G$  ( $s \neq s'$ ) to have equal cosets ( $sH = s'H$ ); indeed, this occurs with any subgroup  $H$  that contains more than one element. Naturally, we list each distinct coset only once in the set  $G/H$ , an idea to which Hölder with his comment about using ‘appropriately chosen elements’ to generate the array. We will explore this essential feature of cosets via specific examples in Tasks 15 – 17 below, and again in Section 5 of this project. Notice also that this set-theoretic definition of  $G/H$  does *not* actually require  $G$  or  $H$  to be finite, and we will consider quotient groups of infinite groups  $G$  in a later task as well.<sup>15</sup> But first, let’s go back to see what Hölder said about how to *multiply* cosets in order to get a group from  $G/H$  in the case where  $H$  is a normal subgroup.

The key to defining the product of two cosets lies in the computation given in the previous excerpt:

$$\begin{array}{lll} s_\nu b_\rho s_\mu b_\sigma & = & s_\nu(b_\rho s_\mu)b_\sigma & \text{where } b_\rho s_\mu \in Hs_\mu \\ & = & s_\nu(s_\mu b_{\rho'})b_\sigma & Hs_\mu = s_\mu H, \text{ by normality of } H \\ & = & (s_\nu s_\mu)(b_{\rho'}b_\sigma) & \text{where } s_\nu s_\mu \in G \text{ and } b_{\rho'}b_\sigma \in H \\ & = & s_x b_\tau. & \end{array}$$

Notice in particular that Hölder has used ‘ $s_x$ ’ to denote the product  $s_\nu s_\mu$ , which we know to be an element of  $G$  by the closure property of groups. Multiplying ‘the horizontal row corresponding to  $s_\nu$ ’ by ‘the horizontal row corresponding to  $s_\mu$ ’ thus produces ‘the horizontal row corresponding to  $s_\nu s_\mu$ .’ In short, the product of two cosets can be defined quite naturally as simply ‘the coset of the product,’ which we can write symbolically as follows:

$$\text{For all } sH, uH \in G/H, (sH)(uH) = (su)H.$$

---

<sup>15</sup>Hölder himself did not look at quotient groups of infinite sets, since the problems that he was attempting to solve required finite groups only.

Before going back to Hölder's discussion of the quotient group, let's take a look at some features of the quotient group  $G/H$  under this definition of coset multiplication, and consider a few examples.

**Task 14** Let  $G$  be a group and  $H$  a normal subgroup of  $G$ . Denote the identity element of  $G$  by  $e$ .

- Show that coset multiplication on  $G/H$  is associative. Begin by assuming  $s, u, y \in G$ . Then compute the products  $[(sH)(uH)](yH)$  and  $(sH)[(uH)(yH)]$ .
- Show that  $H$  is the identity element of  $G/H$ . *Hint:  $eH = H$ .*
- Given  $sH \in G/H$ , how should we define the inverse element  $(sH)^{-1}$ ? Justify your answer.

**Task 15** Let  $G = S_3$  and  $H = A_3$ . Recall (from Section 2) that  $A_3 \triangleleft S_3$ , which allows us to safely proceed with coset multiplication on  $G/H$ .

To simplify notation, let  $\alpha = (1, 3, 2)$ ;  $\beta = (1, 2, 3)$ ;  $\gamma = (2, 3)$ ;  $\delta = (1, 3)$ ;  $\epsilon = (1, 2)$ .

This gives us:  $G = \{1, \alpha, \beta, \gamma, \epsilon, \delta\}$  and  $H = \{1, \alpha, \beta\}$ .

- Explain why there are only two distinct (left) cosets in  $G/H$ :

$$H = \{1, \alpha, \beta\} \quad \text{and} \quad \gamma H = \{\gamma, \epsilon, \delta\}.$$

- Complete the following Cayley table<sup>16</sup> for  $G/H = \{H, \gamma H\}$ .

	$H$	$\gamma H$
$H$		
$\gamma H$		

- What familiar group does  $G/H$  resemble, and in what ways?

[Or, for those who have already studied the concept of a group isomorphism:  
To what familiar group is  $G/H$  isomorphic? Explain how you know.]

**Task 16** Let  $G = \mathbb{Z}_{10}$  and  $H = \{0, 5\}$ . Recall that  $G$  is a group under addition modulo 10.

Since  $G$  is abelian,  $H \triangleleft G$ , which allows us to define coset addition on  $G/H$  as follows:

$$(s + H) + (t + H) = (s + t) + H \quad (\text{where } s, t \in G)$$

- Complete the following list of the five distinct cosets of  $G/H$ :

$$\begin{array}{lll}
 H & = & \{0, 5\} \quad \text{another name for this coset: } 5 + H \\
 1 + H & = & \{1, 6\} \quad \text{another name for this coset: } \underline{\hspace{2cm}} \\
 2 + H & = & \quad \text{another name for this coset: } \underline{\hspace{2cm}} \\
 3 + H & = & \quad \text{another name for this coset: } \underline{\hspace{2cm}} \\
 4 + H & = & \quad \text{another name for this coset: } \underline{\hspace{2cm}}
 \end{array}$$

<sup>16</sup>The Cayley table for  $S_3$  that is included in Appendix II of this project can be used to complete these computations. This is the second table in the Cayley excerpt on page 36. See also Task II.2.

**Task 16 - continued**

(b) Complete the following Cayley table for  $G/H$ :

	$H$	$1 + H$	$2 + H$	$3 + H$	$4 + H$
$H$	$H$	$1 + H$	$2 + H$	$3 + H$	$4 + H$
$1 + H$	$1 + H$				
$2 + H$	$2 + H$				
$3 + H$	$3 + H$				
$4 + H$	$4 + H$				

(c) What familiar group does  $G/H$  resemble, and in what ways?

[Or, for those who have already studied the concept of a group isomorphism:  
To what familiar group is  $G/H$  isomorphic? Explain how you know.]

**Task 17**

Let  $G = \mathbb{Z}$  and  $H = 4\mathbb{Z} = \{4k \mid k \in \mathbb{Z}\}$ .

Since  $G$  is abelian,  $H \triangleleft G$ , which allows us to define coset addition on  $G/H$ .

(a) Show that there are four distinct cosets in  $G/H$  by completing the following list.  
(You do not need to list all the names of each coset!).

$$\begin{aligned}
 H &= \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\} \\
 1 + H &= \{\dots, -11, -7, -3, 1, 5, 9, 13, \dots\} \\
 2 + H &= \\
 3 + H &=
 \end{aligned}$$

(b) Complete the following Cayley table for  $G/H$ :

	$H$	$1 + H$	$2 + H$	$3 + H$
$H$	$H$	$1 + H$	$2 + H$	$3 + H$
$1 + H$	$1 + H$			
$2 + H$	$2 + H$			
$3 + H$	$3 + H$			

(c) What familiar group does  $G/H$  resemble, and in what ways?

[Or, for those who have already studied the concept of a group isomorphism:  
To what familiar group is  $G/H$  isomorphic? Explain how you know.]

As we can see from the example in Task 17, it is possible for an infinite group  $G$  to have just finitely many cosets for a given subgroup  $H$ . In this case, the quotient group itself is also finite. Today, the number of distinct cosets defined by  $H$  is called *the index of  $H$  in  $G$* , and denoted<sup>17</sup>  $(G : H)$ . Notice that, by Lagrange's Theorem, we can also write  $(G : H) = \frac{|G|}{|H|}$  whenever  $G$  is a finite group. (*Why can't we write this when  $G$  is an infinite group?*)

<sup>17</sup>Some textbooks use square brackets instead of parentheses:  $[G : H]$ .

Of course, whether  $G$  is finite or not, each of the distinct cosets in  $G/H$  will have multiple names — a fact that raises a certain quandary about the definition of coset multiplication. Namely, since we are using the names of cosets to define the product, how do we know that the product we obtain does not depend on the particular names that we used to compute it? Or, to phrase the question more formally, how do we know that coset multiplication is *well-defined*? In the next section of the project, we return to our reading of Hölder to see what he has to say about this question. We first bring this section to closure with a task that revisits the method of proving that a subgroup is normal from Task 8, now using the language of cosets and index.

**Task 18** Recall from Task 8 that Netto gave a proof of the following theorem in 1882:

If a group  $G$  of order  $2r$  contains a subgroup  $H$  of order  $r$ , then  $H$  is a normal subgroup of  $G$ .

(a) Restate this theorem using the language of index.

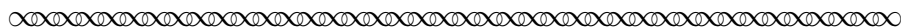
**Theorem** Let  $G$  be a group with  $H$  a subgroup of  $G$ .

If \_\_\_\_\_, then  $H$  is normal in  $G$ .

(b) Recall that Netto's proof of this theorem examined *elements* of the set  $G^{-1}HG$ . Write an alternative proof that does *not* examine specific elements, but instead uses only the language of cosets. That is, show that  $aH = Ha$  for all  $a \in H$ , beginning from the hypothesis you gave to complete the theorem statement in part (a).

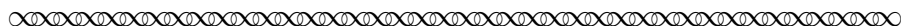
## 5 The Importance of Being Normal

We continue now with our reading of Hölder's paper.



### § 5.

The explanations of the previous paragraphs can also be expressed as follows: One could call two elements from the entire group  $G$  *equivalent*, if they can be conveyed into each other through multiplication by an element of the distinguished (normal) subgroup  $H$ . Due to the interchangeability of the group  $H$  with the elements of the entire group, one need not distinguish in this definition between right and left multiplication. For the same reason, it follows that multiplying equivalents by equivalents yields equivalents. Thus if one partitions the elements of the entire group into classes, such that equivalent elements sit in the same class, and inequivalent elements in different classes, then one obtains a composition of the classes, for which the group property holds. Each  $m$  elements of the original group  $G$  correspond to a specific element of the new group. The composition of elements corresponds between the two groups, that is, there exists between the latter a [surjective] *homomorphism*.<sup>18</sup> This isomorphism is called *merohedral*<sup>19</sup>, because several elements of the first group correspond to one element of the second.



<sup>18</sup>Hölder used the word *isomorphism* here, in keeping with the usage at that time of calling any surjective operation-preserving function by that term. However, the prefix 'iso' has since become associated with only one-to-one functions. To avoid confusion, we have thus employed the current terminology throughout this project.

<sup>19</sup>The word *merohedral* can be read to mean "many-to-one." See the previous footnote for more detail.

**Task 19**

How do the ideas that Hölder described in this excerpt relate to the various specific examples that you examined in the tasks from the previous section? Respond to this question in general first. Then choose one specific example from the previous section, and use it to explain what he meant by each of the following statements in particular.

- One could call two elements from the entire group  $G$  *equivalent*, if they can be conveyed into each other through multiplication by an element of the normal subgroup  $H$ .
- . . . , it follows that multiplying equivalents by equivalents yields equivalents.
- Thus if one partitions the elements of the entire group into classes, such that equivalent elements sit in the same class, and inequivalent elements in different classes, then one obtains a composition of the classes, for which the group property holds.
- Each  $m$  elements of the original group  $G$  correspond to a specific element of the new group.

We will come back to Hölder’s intriguing comments at the end of this excerpt about homomorphisms, and the correspondence which exists between ‘each  $m$  elements of the original group  $G$ ’ and ‘a specific element of the new group’ in the concluding section of this project. Let’s first take a look at what he said about ‘equivalence’ in the first part of this excerpt. There are two basic (but related) ideas here. The first of these is Hölder’s assertion that it is possible to define an *equivalence relationship*<sup>20</sup> on  $G$  by setting  $s \equiv t \bmod H$  if and only if  $(\exists h \in H)(s = th)$ . Recasting this in the language of cosets, this definition becomes  $s \equiv t \bmod H$  if and only if  $s \in tH$ . Hölder further noted that, since  $H$  is normal in  $G$ , its right and left cosets are equal; accordingly, we could also define  $s \equiv t \bmod H$  if and only if  $s \in Ht$ . Of more importance than which of these interchangeable definitions is used for this equivalence relationship, however, is Hölder’s remark that

. . . it follows that multiplying equivalents by equivalents yields equivalents. Thus if one partitions the elements of the entire group into classes, such that equivalent elements sit in the same class, and inequivalent elements in different classes, then one obtains a composition of the classes, for which the group property holds.

In other words, if  $H$  is a normal subgroup of  $G$ , the coset name that we use for each factor doesn’t affect the product itself, so that **coset multiplication is well-defined** in the following sense:

**Given  $s, t, u, v \in G$ , if  $sH = tH$  and  $uH = vH$ , then  $(su)H = (tv)H$ .**

The example in the next task illustrates what goes wrong if we try coset multiplication with a non-normal subgroup. The subsequent task then outlines a proof, using an approach in keeping with Hölder’s remarks from earlier in his paper, that coset multiplication is well-defined for normal subgroups. An alternative approach to proving this important fact is included in Appendix III.

---

<sup>20</sup>Recall that a relationship  $\equiv$  defines an equivalence relationship on a set  $S$  provided it satisfies certain properties that mimic the relationship of equality ( $=$ ). Appendix III examines these properties for the particular equivalence relationship referenced by Hölder in this excerpt through the writings of yet another nineteenth century algebraist, Camille Jordan (1838–1922). Hölder himself simply took this relationship as well-known, due to the work which Jordan and others had done before him within the context of permutation groups.



**Task 20**

Let  $G = S_3 = \{1, \alpha, \beta, \gamma, \epsilon, \delta\}$ , and again employ the notation introduced in Task 15:

$$\alpha = (1, 3, 2), \beta = (1, 2, 3), \gamma = (2, 3), \delta = (1, 3), \epsilon = (1, 2).$$

Consider the subgroup  $K = \langle \gamma \rangle = \{1, \gamma\}$ .

- (a) Complete the following lists of the three distinct left cosets of  $K$ , and the three distinct right cosets of  $K$ . Give all names for each coset.<sup>21</sup>

• $K = 1K = \{1, \gamma\} = \gamma K$	• $K = K1 = \{1, \gamma\} = K\gamma$
• $\alpha K = \{\alpha, \alpha\gamma\} = \{\alpha, \delta\} = \delta K$	• $K\alpha = \{\alpha, \gamma\alpha\} = \{\alpha, \epsilon\} = \underline{\hspace{2cm}}$
• $\beta K = \underline{\hspace{2cm}}$	• $K\beta = \underline{\hspace{2cm}}$

- (b) Use the results from part (a) to explain why  $K$  is not a normal subgroup of  $G$ .

- (c) Compute the following ‘coset products.’

• $\alpha K \beta K = \underline{\hspace{2cm}}$	• $\delta K \epsilon K = \underline{\hspace{2cm}}$
---	--

- (d) Use the results from part (c) to explain why coset multiplication is not well-defined for the non-normal subgroup  $K$ .

**Task 21**

Provide the requested reasons in the first part of the following proof that coset multiplication is well-defined when  $H$  is normal in  $G$ . Then complete the second part of the proof.

**PROOF**

Assume  $H \triangleleft G$ ,  $s, t, u, v \in G$ ,  $sH = tH$  and  $uH = vH$ . We wish to show that  $(su)H = (tv)H$ . We begin by showing that  $(su)H \subseteq (tv)H$ . To this end, let  $x \in (su)H$ . Then there exists  $h \in H$  such that  $x = (su)h$ . Using the fact that  $H$  is normal, we note that  $vH = Hv$ . It follows that:

$$\begin{aligned}
 x &= (su)h \\
 &= s(uh) && \text{by associativity} \\
 &= s(vh_1) && \text{for some } h_1 \in H, \text{ since } \underline{\hspace{2cm}} \\
 &= s(h_2v) && \text{for some } h_2 \in H, \text{ since } \underline{\hspace{2cm}} \\
 &= (sh_2)v && \underline{\hspace{2cm}} \\
 &= (th_3)v && \text{for some } h_3 \in H, \text{ since } \underline{\hspace{2cm}} \\
 &= t(h_3v) && \underline{\hspace{2cm}} \\
 &= t(vh_4) && \underline{\hspace{2cm}} \\
 &= (tv)h_4 && \underline{\hspace{2cm}}
 \end{aligned}$$

Since  $h_4 \in H$  and  $x = (tv)h_4$ , we conclude that  $x \in (tv)H$ . Thus,  $(su)H \subseteq (tv)H$ .

We next show that  $(tv)H \subseteq (su)H$ . \*\*\* Do this!\*\*\*

Having thus shown that both subset relationships hold, we now conclude that  $(st)H = (uv)H$ .

<sup>21</sup>The Cayley table for  $S_3$  that is included in Appendix II of this project can be used to complete these computations. This is the second table in the Cayley excerpt on page 36. See also Task II.2.

Noting that a normal subgroup ensures that coset multiplication is well-defined — or as Hölder expressed it, that **multiplying equivalents by equivalents yields equivalents** — was the key observation needed for him to conclude that:

Thus if one partitions the elements of the entire group into classes, such that equivalent elements sit in the same class, and inequivalent elements in different classes, then **one obtains a composition of the classes, for which the group property holds.**

We highlight this important conclusion in the following formal definition of the quotient group, which we state here for emphasis to summarize the key concepts from this and the preceding section:

**Definition 3**

Let  $G$  be a group and  $H \triangleleft G$ , so that coset multiplication on  $G/H$  is well-defined.

The **quotient group of  $G$  modulo  $H$**  is the set  $G/H = \{sH \mid s \in G\}$  under coset multiplication, with  $H$  as the identity element and  $(sH)^{-1} = s^{-1}H$  for all  $s \in G$ .

Furthermore, the **index of  $H$  in  $G$** , denoted  $(G : H)$ , is defined by  $(G : H) = |G/H|$ .

This formal sounding definition unfortunately loses some of the direct appeal of Hölder's own declaration that 'the group property holds.' In other words:  $G/H$  is itself a GROUP! And as a group, every theorem known to hold for arbitrary groups applies to  $G/H$ , provided we adapt the assumptions of the theorem in question to the quotient group operation of coset multiplication. The closing tasks of this section will provide you with some practice with this type of translation, as well as a glimpse at how the properties of the three distinct groups  $G/H$ ,  $G$  and  $H$  can be related.

**Task 22**

Let  $G$  be a group (not necessarily finite) and  $H \triangleleft G$  with  $(G : H) = m$ , where  $m \in \mathbb{Z}^+$ .

Use theorems about the order of group elements to prove each of the following.

- (a) For all  $a \in G$ ,  $\text{ord}_{G/H}(aH)$  is a divisor of  $m$ .
- (b) For all  $a \in G$ ,  $a^m \in H$ .

**Task 23**

Let  $G$  be a group and  $H \triangleleft G$ .

Use the definition of finite order for group elements to prove the following.

- (a) If every element of  $G/H$  has finite order, and every element of  $H$  has finite order, then every element of  $G$  has finite order.
- (b) If every element of  $G/H$  has finite order, then for every  $a \in G$ , there exists  $n \in \mathbb{Z}$  such that  $a^n \in H$ , and conversely.

**Task 24**

Let  $G$  be a group and  $H \triangleleft G$ . Prove each of the following.

- (a) If  $a^2 \in H$  for every  $a \in G$ , then every element of  $G/H$  is its own inverse, and conversely.
- (b) If there is  $a \in G$  such that for all  $b \in G$ , there exists  $n \in \mathbb{Z}$  with  $ba^n \in H$ , then  $G/H$  is cyclic, and conversely.

**Task 25**

Let  $G$  be a group, and recall that the center of  $G$  is the normal subgroup defined by

$$C = \{x \in G \mid (\forall y \in G)(yx = xy)\}.$$

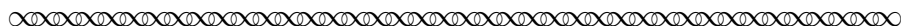
- (a) Prove: If  $G/C$  is cyclic, then  $G$  is abelian.

*Hint: Begin with a generator  $aC$  for the quotient group  $G/C$ , where  $a \in G$ ; then use the definition of generator to show that every  $x \in G$  can be written in the form  $x = ca^n$  for some  $c \in C$  and some  $n \in \mathbb{Z}$ .*

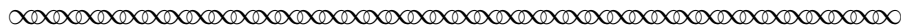
- (b) Give a counterexample to show that the converse of part (a) is not true.

## 6 The Fundamental Homomorphism Theorem

As promised earlier, we now return to the very intriguing comments that Hölder stated at the end of the excerpt in the previous section. Recall first that Hölder had earlier assumed  $H$  is a normal subgroup of the group  $G$ , with  $|H| = m$ .



Each  $m$  [equivalent] elements of the original group  $G$  correspond to a specific element of the new group  $[G/H]$ . The composition of elements corresponds between the two groups, that is, there exists between the latter a [surjective] *homomorphism*. This isomorphism is called *merohedral*<sup>22</sup>, because several elements of the first group correspond to one element of the second.



The first sentence of this excerpt states simply that, given  $|H| = m$ , there is an ‘ $m$ -to-1’ function between the original group  $G$  and the quotient group  $G/H$ . In fact, this is straightforward to see by considering the natural correspondence  $f : G \rightarrow G/H$  defined by  $f(t) = tH$  for each  $t \in G$ . (*Pause here to make sure you see how  $f$  maps  $m$  distinct elements in  $G$  to the same coset in  $G/H$ !*)

It is Hölder’s second statement that may seem surprising to you; namely, that ‘the composition of elements corresponds between the two groups’. Today, we describe this notion by saying that  $f$  *preserves the (group) operation*: given any  $s, t \in G$ ,  $f(st) = f(s)f(t)$ . A function that preserves operations — between any two groups — is also now called a homomorphism. Before we examine Hölder’s claim that the specific function  $f$  between  $G$  and  $G/H$  defined above is a [surjective] homomorphism, let’s take a look at some properties of homomorphisms more generally.

We start with the following formal statement of the terminology involved.

---

<sup>22</sup>Recall that the word *merohedral* can be read to mean “many-to-one.”

**Definition 4**

Let  $(G, *)$  and  $(G', \star)$  be groups with identities 1 and  $1'$  respectively.

- A function  $f : G \rightarrow G'$  is a **homomorphism** from  $G$  to  $G'$  if and only if

$$(\forall s, t \in G)(f(s * t) = f(s) \star f(t)).$$

- Given a homomorphism  $f : G \rightarrow G'$ , the **kernel** and **range** of  $f$  are the sets

$$\text{Ker}(f) = \{s \in G | f(s) = 1'\} \quad \text{and} \quad \text{Ran}(f) = \{y \in G' | (\exists t \in G)(f(t) = y)\}.$$

- $G'$  is a **homomorphic image** of  $G$  if and only if there exists a homomorphism  $f : G \rightarrow G'$  for which  $\text{Ran}(f) = G'$ , or equivalently, if and only if there exists a surjective<sup>23</sup> homomorphism  $f : G \rightarrow G'$ .
- $G$  is **isomorphic to**  $G'$  if and only if there exists a bijective<sup>24</sup> homomorphism  $f : G \rightarrow G'$ .

In the following tasks, we examine some properties and examples of homomorphisms. If you have already studied isomorphic groups, then some of these properties will sound familiar, but with a twist! That twist arises, of course, from the fact that a homomorphism need not be either one-to-one or onto, whereas an isomorphism must be both. For this reason, we will carefully track where and when we use either assumption (one-to-one or onto) in the following tasks.

**Task 26**

Assume that  $(G, *)$  and  $(G', \star)$  are groups with identities 1,  $1'$  respectively.

Let  $f : G \rightarrow G'$  be a group homomorphism.

- Prove that  $H = \text{Ran}(f)$  is a subgroup of  $G'$ . Under what condition will  $H = G'$ ?
- Prove that  $K = \text{Ker}(f)$  is a normal subgroup of  $G$ .

Conclude that  $G/K$  is therefore a quotient group.

**Task 27**

Assume that  $(G, *)$  and  $(G', \star)$  are groups with identities 1,  $1'$  respectively.

Define  $f : G \rightarrow G'$  by  $f(x) = 1'$  for all  $x \in G$ . ( $f$  is called the trivial homomorphism.)

Prove that  $f$  is a homomorphism with  $\text{Ker}(f) = G$ .

Under what conditions will  $f$  be one-to-one? onto?

**Task 28**

Let  $n \in \mathbb{Z}^+$  with  $n \geq 2$ . Define  $f : S_n \rightarrow \mathbb{Z}_2$  by  $f(\sigma) = \begin{cases} 0 & \text{if } \sigma \in A_n \\ 1 & \text{if } \sigma \notin A_n \end{cases}$ .

- Verify that  $f$  is a homomorphism by determining the value of  $f(\sigma\tau)$  and  $f(\sigma)f(\tau)$  for the various cases of parity of  $\sigma$  and  $\tau$ . (There are three cases in all: both even, both odd, one even/one odd). Explain how this shows that  $\mathbb{Z}_2$  is a homomorphic image of  $S_n$ .
- Also explain why  $\text{Ker}(f) = A_n$ . Since  $A_n \triangleleft S_n$  (give two reasons why we know this!), the quotient group  $S_n/A_n$  is defined. To what familiar group is  $S_n/A_n$  isomorphic? Justify your response.

<sup>23</sup>Recall that a surjective function is onto:  $(\forall y \in G')(\exists s \in G)(f(s) = y)$ .

<sup>24</sup>Recall that a bijective function is both surjective and injective.

Further recall that an injective function is one-to-one:  $(\forall s, t \in G)(f(s) = f(t) \Rightarrow s = t)$ .

**Task 29**

Assume that  $(G, *)$  and  $(G', \star)$  are groups with identities  $1, 1'$ , respectively.

Let  $f : G \rightarrow G'$  be a group homomorphism.

- (a) Prove that  $f(1) = 1'$  by showing that  $f(1) \star y = y \star f(1) = y$  for all  $y \in G'$ .

This shows that identities are preserved by all group homomorphisms.

- (b) Given  $x \in G$ , prove that  $[f(x)]^{-1} = f(x^{-1})$  by showing that  $f(x^{-1}) \star f(x) = 1'$ .

This shows that inverses are preserved by all group homomorphisms.

- (c) Assume  $x \in G$  has finite order  $r$ .

Prove  $\text{ord}_{G'}[f(x)]$  divides  $\text{ord}_G(x)$  by showing  $[f(x)]^r = 1'$ .

Then give an example to show  $\text{ord}_{G'}[f(x)] < \text{ord}_G(x)$  is possible when  $f$  is not onto.

*Optional:*

Complete the proof that  $\text{ord}_{G'}[f(x)] = \text{ord}_G(x)$  for every  $x \in G$  in the case where  $G'$  is a homomorphic image of  $G$ . Indicate clearly where the additional assumption that  $f$  is onto is used.

- (d) Prove: If  $G$  is abelian, then  $\text{Ran}(f)$  is also abelian.

Use this to conclude that the homomorphic image of an abelian group is also abelian.

Then give an example to show  $G'$  can be non-abelian, even if  $G$  is abelian.

*Optional:*

Complete the proof that  $G$  is abelian if and only if  $G'$  is abelian in the case where  $f$  is an isomorphism. Indicate clearly where the additional assumptions that  $f$  is both one-to-one and onto are used.

- (e) Prove: If  $G$  is cyclic, then  $\text{Ran}(f)$  is also cyclic.

Use this to conclude that the homomorphic image of a cyclic group is also cyclic.

Then give an example to show  $G'$  can be non-cyclic, even if  $G$  is cyclic.

*Optional:*

Complete the proof that  $G$  is cyclic if and only if  $G'$  is cyclic in the case where  $f$  is an isomorphism. Is it necessary for  $f$  to be both one-to-one and onto in your proof? Explain why or why not.

**Task 30**

Consider the function  $f : \mathbb{Z}_8 \rightarrow \mathbb{Z}_4$  defined by  $f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 \end{pmatrix}$ .

- (a) Verify that  $f$  is a homomorphism by checking that  $f$  transforms the Cayley table of  $\mathbb{Z}_8$  to the Cayley table of  $\mathbb{Z}_4$ ,

Table for  $\mathbb{Z}_8$ 

	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Transformed Table for  $f[\mathbb{Z}_8]$ 

	0	1	2	3	0	1	2	3
0	0	1	2	3	0	1	2	3
1	1							
2	2							
3	3							
0	0							
1	1							
2	2							
3	3							

Transformed Table for  $f[\mathbb{Z}_8]$  with duplicates removed:

	0	1	2	3
0	0	1	2	3
1	1			
2	2			
3	3			

- (b) Let  $K = \text{Ker}(f)$ . Find the elements of  $K$ , and then also find the remaining (three) LEFT cosets of  $K$ . (Each coset in this example will have two ‘names’; give both!)
- (c) What do you notice about the relationship of the function images of elements that come from the same coset? That is, for each of the distinct cosets  $a + K$ , what do you notice about  $f(x)$  when  $x \in a + K$ ?

**Task 31**

Consider the function  $f : \mathbb{Z}_8 \rightarrow \mathbb{Z}_4$  defined by  $f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 \end{pmatrix}$

Given that  $f$  is a homomorphism, find  $K = \text{Ker}(f)$ .

Verify that  $(G : K) = 4$ , and list the elements of each the four cosets  $a + K$ .

What do you notice about the relationship of the function images of elements that come from the same coset? To what familiar group is  $\mathbb{Z}_8/K$  isomorphic?

**Task 32**

- (a) Find the homomorphism  $f : \mathbb{Z}_{15} \rightarrow \mathbb{Z}_5$  obtained by setting  $f(1) = 1$ .  
(You do NOT need to verify that it's a homomorphism.)

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 0 & 1 & & & & & & & & & & & & & \end{pmatrix}$$

Also find  $K = \text{Ker}(f)$ , and list all cosets of  $K$ .

What do you notice about the relationship of the function images of elements that come from the same coset?

To what familiar group is  $\mathbb{Z}_{15}/K$  isomorphic?

- (b) Now find a second homomorphism  $g : \mathbb{Z}_{15} \rightarrow \mathbb{Z}_5$  by setting  $g(1) = 3$ .  
(You do NOT need to verify that it's a homomorphism.)

$$g = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 0 & 3 & & & & & & & & & & & & \end{pmatrix}$$

Also find  $K = \text{Ker}(g)$ , and list all cosets of  $K$ . What do you notice about the relationship of the function images of elements that come from the same coset?

To what familiar group is  $\mathbb{Z}_{15}/K$  isomorphic?

The following general theorem reflects the observations you made in the three previous tasks.

**Theorem 1**

Let  $f : G \rightarrow G'$  be a homomorphism with  $\text{Ker}(f) = K$ . Let  $a, b \in G$ .

Then  $f(a) = f(b)$  if and only if  $b \in aK$ .

We will make use of this theorem later in this section. First, take a look at the next two tasks, which request a proof and an application of Theorem 1, respectively.

**Task 33**

- (a) Prove Theorem 1.  
(b) Prove the following corollary to Theorem 1:

Let  $f : G \rightarrow G'$  be a homomorphism with  $\text{Ker}(f) = K$ .

Then  $f$  is 1-to-1 if and only if  $\text{Ker}(f) = \{1\}$ .

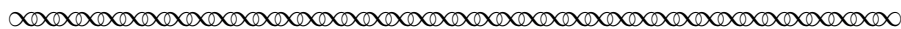
**Task 34**

Let  $f : \mathbb{Z}_{15} \rightarrow \mathbb{Z}_{10}$  be a homomorphism with  $K = \text{Ker}(f) = \{0, 5, 10\}$ .

Suppose that  $f(3) = 8$ .

- (a) Use Theorem 1 to find all  $x \in \mathbb{Z}_{15}$  such that  $f(x) = 8$ .  
(Remember to first re-write Theorem 1 using additive notation.)  
(b) Determine the value of  $f(6)$ . Then find all  $x \in \mathbb{Z}_{15}$  such that  $f(x) = f(6)$ .  
Indicate your reasoning briefly.  
(c) Determine the value of  $f(14)$ . Then find all  $x \in \mathbb{Z}_{15}$  such that  $f(x) = f(14)$ .  
Indicate your reasoning briefly.  
(d) Find  $\text{Ran}(f)$ , justifying your response.

Let's now go back to read Hölder's comments about the relationship between quotient groups and homomorphisms. Recall again that Hölder had earlier assumed  $H$  is a normal subgroup of the group  $G$ , with  $|H| = m$ .



Each  $m$  elements of the original group  $G$  correspond to a specific element of the new group  $[G/H]$ . The composition of elements corresponds between the two groups, that is, there exists between the latter a [surjective] *homomorphism*. This isomorphism is called *merohedral*<sup>25</sup>, because several elements of the first group correspond to one element of the second.



Re-writing this in the current language of homomorphisms, we get the following.

### Theorem 2

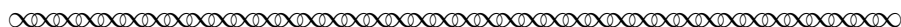
Let  $H \triangleleft G$  and define  $f : G \rightarrow G/H$  by  $f(a) = aH$ .

Then  $f$  is a homomorphism onto  $G/H$ . Furthermore,  $H = \text{Ker}(f)$ .

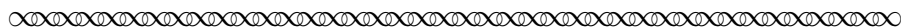
### Task 35

Prove Theorem 2.

Theorems 1 and 2 may seem quite natural after working the examples in the previous tasks. But notice what Hölder said next:



In all cases the order of the group  $G$  equals the product of the orders of the groups  $G/H$  and  $H$ . One can also say, that the group  $G$  is split into two factors. Here's an example.<sup>§</sup> The factors play a different role in the process. Hence the group  $G/H$  may always be construed as the first factor, which is [a homomorphic image of] the group  $G$ , and the group  $H$  construed as the second factor, which is a distinguished (maximal) subgroup of  $G$ . The distinguished (normal) subgroup here forms the starting point, but **one could also proceed from the [surjective] homomorphism**. Here's an example.<sup>¶</sup>



<sup>25</sup>Recall that the word *merohedral* can be read to mean “many-to-one.”

<sup>§</sup>Hölder's footnote: Cf. Dyck, Grouptheoretic studies, *Math. Ann.* vol. 20, p. 14.

<sup>¶</sup>Hölder's footnote: Cf. Dyck, Grouptheoretic studies, these *Ann.* vol. 20, p. 14.



This brings us to the pièce de resistance of Hölder’s paper! Not only does every normal subgroup of  $G$  give us a quotient group that is a homomorphic image of  $G$ , but every homomorphic image of  $G$  also corresponds to a normal subgroup of  $G$ !! Today, this latter result is known as the Fundamental Homomorphism Theorem. Using the symbol ‘ $\cong$ ’ to denote ‘is isomorphic to,’ we can state this important theorem as follows:

**Theorem 3: The Fundamental Homomorphism Theorem:**

If  $f : G \rightarrow G'$  is a group homomorphism from  $G$  onto  $G'$  with  $\text{Ker}(f) = K$ , then

$$G/K \cong G'.$$

Given your work with the various examples in the project, the idea behind this powerful theorem may seem fairly natural. Before looking at the details of the formal proof of the Fundamental Homomorphism Theorem, let’s take a look at some tasks that illustrate it in a different way, and also begin to reveal some of its power. First, take a look at the following diagram, which captures the essence of both the theorem, and its proof.

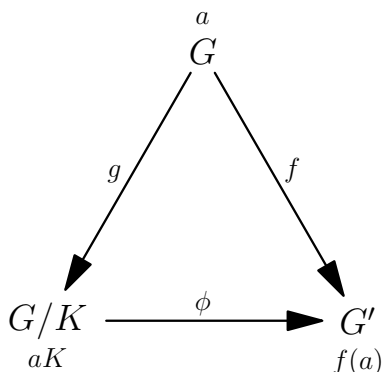


Figure 1: Diagram of the Fundamental Homomorphism Theorem

**Task 36**

Using ‘ $\text{Dom}(f)$ ’ to denote the domain of the function  $f$ , here is a useful way to think about what the Fundamental Homomorphism Theorem says:

$$\text{Dom}(f)/\text{Ker}(f) \cong \text{Ran}(f) \text{ whenever } f \text{ is a group homomorphism.}$$

Explain clearly how this version of the Fundamental Homomorphism Theorem corresponds to the formal statement given in Theorem 3.

**Task 37** Let  $G, H$  be groups with  $G$  finite and assume  $f : G \rightarrow H$  is a homomorphism.

Use the Fundamental Homomorphism Theorem to explain why  $|\text{Ker}(f)|$  and  $|\text{Ran}(f)|$  are both divisors of  $|G|$ . Give an example to show that  $H$  need not be finite.

**Task 38** Consider the subgroup  $K = \langle (1, 1) \rangle = \{(0, 0), (1, 1), (2, 2)\}$  of the abelian group  $\mathbb{Z}_3 \times \mathbb{Z}_3$ . Use the Fundamental Homomorphism Theorem to prove that  $\mathbb{Z}_3 \cong (\mathbb{Z}_3 \times \mathbb{Z}_3)/K$ .

Do this by finding a function  $f : \mathbb{Z}_3 \times \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$  with  $\text{Ker}(f) = K$

**Task 39** (a) Use the Fundamental Homomorphism Theorem to prove the following:

If  $G$  is a group with normal subgroups  $H, K$  and  $H \subseteq K$ , then  $\frac{G/H}{K/H} \cong G/K$ .

*Hint: What is the most natural way to define a function  $f : G/H \rightarrow G/K$ ?*

- (b) Use part (a) to show that  $\frac{G/H}{K/H} \cong \mathbb{Z}_4$ , where  $G = \mathbb{Z}_{24}$ ,  $H = \langle 12 \rangle$  and  $K = \langle 4 \rangle$ . Be sure to explain how you know that we obtain a **cyclic** group by indicating its generators.

**Task 40** (a) Let  $G_1, G_2$  be groups with  $J_1 \triangleleft G_1$  and  $J_2 \triangleleft G_2$ .

Verify that  $(G_1 \times G_2)/(J_1 \times J_2)$  is a group by showing that  $J_1 \times J_2 \triangleleft G_1 \times G_2$ .

- (b) Use the Fundamental Homomorphism Theorem to prove the following:

If  $G_1, G_2$  are groups with  $J_1 \triangleleft G_1$  and  $J_2 \triangleleft G_2$ , then

$$(G_1 \times G_2)/(J_1 \times J_2) \cong (G_1/J_1) \times (G_2/J_2)$$

*Hint: Consider the function  $f : G_1 \times G_2 \rightarrow (G_1/J_1) \times (G_2/J_2)$  defined by  $f((x, y)) = (xJ_1, yJ_2)$  for all  $(x, y) \in G_1 \times G_2$ .*

- (c) Consider the group  $G = \mathbb{Z}_9 \times \mathbb{Z}_6$  and subgroup  $H = \langle 3 \rangle \times \langle 3 \rangle$ .

Use part (a) to determine the familiar group to which  $G/H$  is isomorphic.

**Task 41**

Complete the following proof sketch for the Fundamental Homomorphism Theorem.

Let  $G, G'$  be groups,  $G'$  a homomorphic image of  $G$  and  $f : G \rightarrow G'$  a homomorphism of  $G$  onto  $G'$  with  $\text{Ker}(f) = K$ . We wish to show  $G/K \cong G'$ . To this end, define  $\phi : G/K \rightarrow G'$  by  $\phi(Ka) = f(a)$ . Assume  $a, b \in G$  arbitrary. We must show:

(a)  $\phi$  is well defined: *If  $Ka = Kb$ , then  $\phi(Ka) = \phi(Kb)$ .*

Assume  $Ka = Kb$ . Then

$$\begin{aligned}\phi(Ka) &= f(a) && \text{by definition of } \phi \\ &= f(b) && \text{by Theorem 1 } (K = \text{Ker}(f)) \text{ and the assumption that } Ka = Kb \\ &= \phi(Kb) && \text{by } \underline{\hspace{10em}}\end{aligned}$$

(b)  $\phi$  is one-to-one: *If  $\phi(Ka) = \phi(Kb)$ , then  $Ka = Kb$ .*

Assume  $\phi(Ka) = \phi(Kb)$ .

Then  $f(a) = f(b)$  since  $\phi(Ka) = f(a)$  and  $\phi(Kb) = f(b)$  (by definition of  $\phi$ )

Thus,  $Ka = Kb$  by  $\underline{\hspace{10em}}$

(c)  $\phi$  is onto: *For every  $y \in G'$ , there exists  $Ka \in G/K$  such that  $\phi(Ka) = y$ .*

Assume  $y \in G'$ . Note that  $G' = \text{Ran}(f)$  since  $\underline{\hspace{10em}}$ .

Thus, there exist  $a \in \underline{\hspace{2em}}$  such that  $f(a) = y$  by definition of  $\underline{\hspace{2em}}$ .

Note that  $Ka \in \underline{\hspace{2em}}$ .

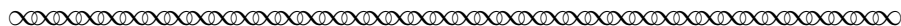
Furthermore, by definition of  $\phi$ , we have  $\phi(Ka) = \underline{\hspace{2em}} = y$ .

(d)  $\phi$  preserves operation:  $\phi(KaKb) = \phi(Ka)\phi(Kb)$

Observe that

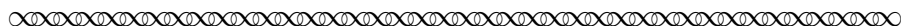
$$\begin{aligned}\phi(KaKb) &= \phi(K(ab)) && \text{by } \underline{\hspace{10em}} \\ &= f(ab) && \text{by } \underline{\hspace{10em}} \\ &= f(a)f(b) && \text{since } \underline{\hspace{10em}} \\ &= \phi(Ka)\phi(Kb) && \text{by } \underline{\hspace{10em}}\end{aligned}$$

In his final comments about the general concept of a quotient group, Hölder hinted at an intriguing relationship between properties of the quotient group  $G/H$ , the original group  $G$  and the normal subgroup  $H$ .



In all cases the order of the group  $G$  equals the product of the orders of the groups  $G/H$  and  $H$ . One can also say, that the group  $G$  is split into two factors. Here's an example.\*\* The factors play a different role in the process. Hence the group  $G/H$  may always be construed as the first factor, which is a [homomorphic image] of the group  $G$ , and the group  $H$  construed as the second factor, which is a distinguished (normal) subgroup of  $G$ .

To the problem of splitting a group into two factors, one can pose to oneself the converse: Given two groups as factors, from these piece together a group as the product. This problem sometimes admits multiple solutions, I hope to treat this on another occasion.



Hölder himself continued this particular paper by applying the quotient group concept to solve another problem in group theory. This latter problem goes beyond the scope of this project, as does the converse splitting problem that Hölder posed at the end of this last excerpt. We thus bring our study of quotient groups in this project to an end with two examples that show how a group  $G$  can be 'split into'  $G/H$  and  $H$  which represent distinct aspects of  $G$ , by 'factoring out' all the elements of  $G$  with a particular property.

#### Task 42

In this task, you will prove that 'factoring out' all the elements of  $G$  that have finite order results in a factor group  $G/H$  that has only one element of finite order.

Let  $G$  be an abelian group and  $H \triangleleft G$ . Assume that  $H$  contains all elements of  $G$  that have finite order. Prove that no non-identity element of  $G/H$  has finite order.

Do this by assuming  $aH \in G/H$  has finite order, where  $a \in G$ ; then prove  $aH = H$ .

#### Task 43

Recall that a *commutator* of a group  $G$  is any element of the form  $xyx^{-1}y^{-1}$ , where  $x, y \in G$ .

- (a) Let  $H$  be a subgroup of  $G$  and assume that  $H$  contains all the commutators of  $G$ .

Recall from Task 7 that  $H$  is therefore normal in  $G$ , so that we can form the quotient group  $G/H$ . Prove that  $G/H$  is abelian.

- (b) Notice that the number of distinct commutators is a measure of the degree to which  $G$  is non-abelian; for instance, every abelian group has only the identity as its single commutator. Explain how part (a) shows that factoring out the commutators from a group results in an abelian quotient group.

---

\*\*Hölder's footnote: Cf. Dyck, Grouptheoretic studies, Math. Ann. vol. 20, p. 14.

## References

- Augustin Cauchy. 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. *Journal de l'École Polytechnique*, 17(10):1–28, 1815a. Also in *Œuvres complètes de Augustin Cauchy*, Série 2, Tome 1 (1905), 64–90.
- Augustin Cauchy. 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. *Journal de l'École Polytechnique*, 17(10):29–117, 1815b. Also in *Œuvres complètes de Augustin Cauchy*, Série 2, Tome 1 (1905), 91–169.
- Arthur Cayley. On the theory of groups, as depending on the symbolic equation  $\theta^n = 1$  - part i. *Philosophical Magazine*, 7:40–47, 1854. Also in *The Collected Mathematical Papers of Arthur Cayley*, Cambridge: Cambridge University Press, vol. 2 (1889), 123–130.
- Arthur Cayley. On the theory of groups, as depending on the symbolic equation  $\theta^n = 1$  - Part III. *Philosophical Magazine*, 18:34–37, 1859. Also in *The Collected Mathematical Papers of Arthur Cayley*, Cambridge: Cambridge University Press, vol. 2 (1889), 594–602.
- Sujoy Chakraborty and Munibur Rahman Chowdhury. Arthur Cayley and the Abstract Group Concept. *Mathematics Magazine*, 78(4):269–282, October 2005.
- Otto Hölder. Zurückführung einer beliebigen algebraischen Gleichung auf eine Kette von Gleichungen (Reduction of an arbitrary algebraic equation to a chain of equations). *Mathematische Annalen*, 34:26–56, 1889.
- Camille Jordan. Sur la limite de transitivité des groupes non alternés (On the limits of transitivity in non-alternating groups). *Bulletin de la Société Mathématique Française*, 1:40–71, 1872–1873.
- Eugen Netto. *Substitutionentheorie und ihre Anwendungen auf die Algebra*. Teubner, Leipzig, 1882.
- David Pengelley. Quick, Does  $23/67$  Equal  $33/97$ ? A Mathematician's Secret from Euclid to Today. *American Mathematical Monthly*, 120(10):67–876, December 2013.
- Richard L. Roth. A history of Lagrange's theorem on groups. *Mathematics Magazine*, 74(2):99–108, April 2001.

## APPENDIX I: Cauchy's Proof of Lagrange's Theorem for Permutation Groups<sup>26</sup>

In his initial description of the quotient group defined by a normal subgroup (Section 4 of this project), Hölder remarked that the array scheme he was employing had already been used in Augustin Cauchy's<sup>27</sup> proof of a certain theorem. This appendix presents Cauchy's original proof of that theorem, which you will have already encountered (stated for groups in general) under the name *Lagrange's Theorem*.<sup>28</sup> Although Cauchy was thinking only of permutation groups<sup>29</sup> at the time, his proof strategy works perfectly well for abstract groups. In fact, the proof strategy found in most of today's textbooks, while phrased in the language of cosets, is strongly reminiscent of Cauchy's approach. We will say more about the modern statement of the theorem and its proof below. But first, begin by reading (and re-reading!) Cauchy's proof of Lagrange's Theorem (for permutation groups), as well as the comments on his strategy that follow this excerpt. As you do so, also consider how Cauchy's notation and presentation of the array is similar to, and different from, that given by Hölder on page 10 of this project.

**Before reading Cauchy's proof**, take note of the following conventions that he had introduced in an earlier excerpt from his *Exercices d'analyse et de physique mathématique* [Cauchy, 1815a].

- A 'system of conjugate permutations' is a finite set of permutations that is closed under permutation products; since permutation multiplication is associative, this implies that any 'system of conjugate permutations' is a group (or subgroup) of permutations (as noted by Hölder in Section 1 of this project).
- Series (1) designates the system of *all* possible  $N = n!$  permutations on  $n$  letters; that is, Series (1) is the permutation group  $S_n$ .
- Series (2) designates an arbitrary system of conjugate permutations (or subgroup of  $S_n$ ) on  $n$  variables, with the individual permutations in the series denoted as  $1, P, Q, R \dots$

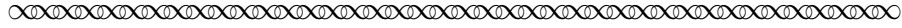
---

<sup>26</sup>The proof and related tasks in this appendix are drawn from another of the author's primary source projects, *Abstract Awakenings in Group Theory*, which explores elementary group theory through the writings of Lagrange, Cauchy and Cayley. To obtain the current version of that project, contact the author at [janet.barnett@csupueblo.edu](mailto:janet.barnett@csupueblo.edu), or visit [www.cs.nmsu.edu/historical-projects/projects.php](http://www.cs.nmsu.edu/historical-projects/projects.php) for an earlier version.

<sup>27</sup>Augustin 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 Lagrange, 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. 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. 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.

<sup>28</sup>The name of J. L. Lagrange (1736–1813) is associated with this theorem due to a related result that Lagrange stated prior to Cauchy's work in permutation theory, but within the (more limited) context of the number of forms resulting from permutations of variables of a function. For more on this history, see [Roth, 2001].

<sup>29</sup>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. (See [Cauchy, 1815a,b] in the bibliography for their titles.) 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.



*Theorem*<sup>30</sup> 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  $U, V, W, \dots$  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

$$(5) \quad 1, U, V, W, \dots$$

then the table

$$(6) \quad \begin{cases} 1, & P, & Q, & R, & \dots \\ U, & UP, & UQ, & UR, & \dots \\ V, & VP, & VQ, & VR, & \dots \\ W, & WP, & WQ, & WR, & \dots \\ \text{etc,} \end{cases}$$

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

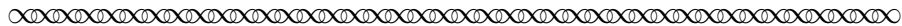
$$V = US,$$

$S = PQ^{-1}$  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  $N$ .




---

<sup>30</sup>All translations into English from Cauchy's paper are due to the project author.

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 every element is placed in some row of the table in such a way 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 I.1 below outlines the construction of a table satisfying these two conditions in a very specific case. Task I.2 then asks you to re-write Cauchy's proof using the current terminology of permutation groups. The following list summarizes once more how this terminology is related to that of Cauchy.

- The ***symmetric group***  $S_n$  is the set of all permutations on  $n$  objects.
  - This is what Cauchy called (somewhat long-windedly):  
'the system of all permutations that one can form with  $n$  letters  $x, y, z \dots$ '.
  - In Cauchy's proof of Theorem 1, series (1) lists the elements of  $S_n$ .
  - The order of  $S_n$  is  $n!$ .
- A ***subgroup of***  $S_n$  is a non-empty subset  $H \subseteq S_n$  which is closed under products; since  $H$  is necessarily finite, it is also therefore closed under inverses.
  - 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  $H$ .
  - $S_n$  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 I.1

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:

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

- (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:

$$(\alpha) \quad r_4 h_3 \neq r_4 h_4$$

$$(\beta) \quad r_3 h_3 \neq r_4 h_3$$

$$(\gamma) \quad r_4 h_3 \neq r_2 h_4$$

**Note:** Part  $(\gamma)$  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, but may do so if you wish.)

$h_1 = 1$	$h_2 = (x, y, z, u)$	$h_3 = (x, z)(y, u)$	$h_4 = (x, u, z, y)$
$r_2 = (x, y)$	$r_2 h_2 = (x, y)(x, y, z, u)$ $= (y, z, u)$	$r_2 h_3 = (x, y)(x, z)(y, u)$ $= (x, z, y, u)$	$r_2 h_4 = (x, y)(x, u, z, y)$ $= (x, u, z)$
$r_3 = (x, z)$	$r_3 h_2 = (x, z)(x, y, z, u)$ $=$	$r_3 h_3 = (x, z)(x, z)(y, u)$ $=$	$r_3 h_4 = (x, z)(x, u, z, y)$ $=$
$r_4 = (x, u)$			

- (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?

### Task I.2

Write a fully general rigorous proof of Lagrange's Theorem for an arbitrary finite group  $G$ , but using Cauchy's strategy of building an array in which all elements of  $G$  appear exactly once. In order to do this in full generality, you should introduce indexed variables to denote the elements of the subgroup  $H$ , as well as for the first element of each row of the array. (See Task I.1.) It will also be useful to use coset notation to represent each row of the array. After formally (and carefully) using recursion to define the array, explicitly prove that the completed array satisfies the following two conditions:

- (i) no row (or coset) contains repeated elements ; and
- (ii) no element of a given row (or coset) appears in some earlier row (or coset).

Also add detail and/or rephrase Cauchy's reasoning where you feel this is needed and/or helpful.

## APPENDIX II: Cayley’s Classification of Groups of Small Order<sup>31</sup>

In the closing section of the inaugural paper on abstract groups, Arthur Cayley<sup>32</sup> began the task of classifying all groups of finite order [Cayley, 1854]. Having proven that all groups of prime order are necessarily cyclic, Cayley knew that there is only one group (up to isomorphism) of order  $p$  for any given prime  $p$ . When  $n$  is composite, however, a group of order  $n$  can be cyclic, but is not necessarily so. The problem that Cayley thus took up at this point of his paper was that of identifying all possible non-isomorphic groups of order  $n$  for various composite values of  $n$ . If these distinct non-isomorphic group structures could be fully identified, they would in turn serve as prototypes for all groups of that same order, much as  $\mathbb{Z}_p$  serves as the prototypical group of order  $p$  when  $p$  is prime. That is, any group of order  $n$  would be isomorphic to one of the distinct prototypical structures available for that order.

In his 1854 paper, Cayley succeeded in classifying all groups of order  $n = 4$  and  $n = 6$ ; in his later paper [Cayley, 1859]), he also gave the classification of groups of order  $n = 8$ . In time, it became clear that the problem of classifying *all* groups of finite order is (very!) difficult — so much so that mathematicians eventually turned to the (presumably more straightforward) task of classifying certain types of finite groups. *Simple groups* were considered especially important in this regard, due to the special role they play within group theory: much as prime numbers serve as the basic building blocks of all natural numbers, simple groups serve as the basic building blocks of all groups. Simple groups are today defined as those with only two normal subgroups: the trivial subgroup and the group itself. The underlying concept itself can be traced back to Galois’s work on algebraic solvability.

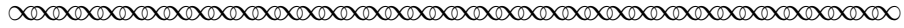
The first major results related to the classification of finite simple groups were published in 1870 by Camille Jordan (1838–1922). Yet it was not until 1981, after a coordinated effort by over 100 different mathematicians beginning in 1965, that the search for all finite simple groups was declared complete. Even then, gaps initially remained in the proof — as might well be expected with a proof that stretched out over approximately 500 journal articles totaling 10,000–15,000 pages. Known as the ‘Enormous Theorem,’ the full Classification of Finite Simple Groups Theorem is now considered by experts to be fully established. The publication of a revised ‘second generation proof’ currently under way by the American Mathematical Society is expected to fill approximately twelve volumes and 3000–4000 pages.

The excerpt on the next page presents the conclusion of Cayley’s analysis of all groups of order 6, in which he established that there are only two such groups, with the Cayley tables given below.

---

<sup>31</sup>The material presented in this appendix is drawn from another of the author’s primary source projects, *Abstract Awakenings in Group Theory*, which explores elementary group theory through the writings of Lagrange, Cauchy and Cayley. To obtain the current version of that project, contact the author at [janet.barnett@csupueblo.edu](mailto:janet.barnett@csupueblo.edu), or visit [www.cs.nmsu.edu/historical-projects/projects.php](http://www.cs.nmsu.edu/historical-projects/projects.php) for an earlier version.

<sup>32</sup>Born in England in 1821, Arthur Cayley and his parents lived in St. Petersburg, Russia during the first eight years of his childhood before returning to England to live near London. Cayley began publishing research papers in mathematics while still an undergraduate at Trinity College, Cambridge. Following his graduation in 1842, he taught as a Fellow at Cambridge for four years before training as a lawyer to secure a means of support. Admitted to the bar in 1849, Cayley worked as a lawyer for 14 years while continuing his mathematical research. Despite a significant decrease in income, Cayley left the legal profession in 1863 to accept an appointment as Sadleirian professor of Pure Mathematics at Cambridge, thereafter devoting his professional life to mathematical research until his death at his home in Cambridge after a long period of suffering. Cayley’s mathematical interests were strongly influenced by the general state of British mathematics at the time, and especially the concept of a ‘symbolical algebra’ in which one begins with formal laws for a given set of symbols and operations on those symbols and only later interprets these as having particular meaning, in contrast to ‘arithmetical algebra,’ which derives its laws from the actual meaning of operations on numbers. Alongside his collaborator J. J. Sylvester (1814–1897), Cayley is widely recognized as one of the founders of matrix theory. In addition to his contributions to algebra, which include both the first paper ever written on matrix theory and the first paper ever written on group theory, his 900+ papers and notes include publications on nearly every aspect of modern mathematics.



If we represent the first of these two forms, viz. the group

$$1, \alpha, \alpha^2, \gamma, \alpha\gamma, \alpha^2\gamma, (\alpha^3 = 1, \gamma^2 = 1, \gamma\alpha = \alpha\gamma),$$

by the general symbols

$$1, \alpha, \beta, \gamma, \delta, \epsilon,$$

we have the table

	1	$\alpha$	$\beta$	$\gamma$	$\delta$	$\epsilon$
1	1	$\alpha$	$\beta$	$\gamma$	$\delta$	$\epsilon$
$\alpha$	$\alpha$	$\beta$	$\gamma$	$\delta$	$\epsilon$	1
$\beta$	$\beta$	$\gamma$	$\delta$	$\epsilon$	1	$\alpha$
$\gamma$	$\gamma$	$\delta$	$\epsilon$	1	$\alpha$	$\beta$
$\delta$	$\delta$	$\epsilon$	1	$\alpha$	$\beta$	$\gamma$
$\epsilon$	$\epsilon$	1	$\alpha$	$\beta$	$\gamma$	$\delta$

while if we represent the second of these two forms, viz. the group

$$1, \alpha, \alpha^2, \gamma, \alpha\gamma, \alpha^2\gamma, (\alpha^3 = 1, \gamma^2 = 1, \gamma\alpha = \alpha^2\gamma),$$

by the general symbols

$$1, \alpha, \beta, \gamma, \delta, \epsilon,$$

we have the table

	1	$\alpha$	$\beta$	$\gamma$	$\delta$	$\epsilon$
1	1	$\alpha$	$\beta$	$\gamma$	$\delta$	$\epsilon$
$\alpha$	$\alpha$	$\beta$	1	$\delta$	$\epsilon$	$\gamma$
$\beta$	$\beta$	1	$\alpha$	$\epsilon$	$\gamma$	$\delta$
$\gamma$	$\gamma$	$\epsilon$	$\delta$	1	$\beta$	$\alpha$
$\delta$	$\delta$	$\gamma$	$\epsilon$	$\alpha$	1	$\beta$
$\epsilon$	$\epsilon$	$\delta$	$\gamma$	$\beta$	$\alpha$	1

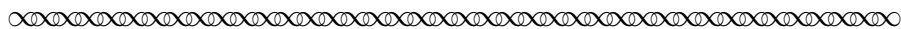
An instance of a group of this kind is given by the permutation of three letters; the group

$$1, \alpha, \beta, \gamma, \delta, \epsilon,$$

may represent a group of substitutions<sup>33</sup> as follows:

$$\begin{array}{cccccc} abc, & abc, & abc, & abc, & abc, & abc, \\ abc & cab & bca & acb & cba & bac \end{array}$$

Another singular instance is given by the optical theorem proved in my paper “On a property of the Caustic<sup>34</sup> by refraction of a Circle, . . . .”



### Task II.1

In this task, we translate the permutations of three letters defined by Cayley in the last excerpt into the notation of  $S_3$ .

For example, letting  $a = 1$ ,  $b = 2$  and  $c = 3$ , the permutation  $\alpha$  which Cayley denoted simply by the two rows  $\begin{array}{c} abc \\ cab \end{array}$  corresponds to the cycle  $\alpha = \begin{pmatrix} 123 \\ 312 \end{pmatrix} = (1, 3, 2)$ .

- (a) Write the permutations denoted by Cayley as  $\beta, \gamma, \delta$  and  $\epsilon$  as cycles in  $S_3$ .
- (b) Use cycle multiplication to verify the row corresponding to  $\alpha$  in the Cayley table. That is, verify that  $\alpha^2 = \beta$ ,  $\alpha\beta = 1$ , etc. using the cycles of  $S_3$  denoted by  $1, \alpha, \beta, \gamma, \delta, \epsilon$ .

### Task II.2 Let $H = \langle \alpha \rangle$ .

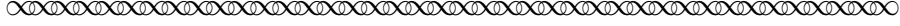
- (i) Use the Cayley table for  $S_3$  on the preceding page to verify that  $H = \{1, \alpha, \beta\}$  and  $\gamma H = \{\gamma, \epsilon, \delta\}$ .
- (ii) Describe where  $H, \gamma H$  show up in the Cayley table of  $S_3$ .  
What do you notice about the way Cayley presented  $H$  and  $\gamma H$  in this table?  
Explain in particular how the pattern formed by the double lines in this Cayley table relates to the quotient group  $G/H$ .

<sup>33</sup>Cayley’s actual notation for substitutions (i.e., permutations) was a variation of the notation in use today (which was first introduced by Cauchy); we have modified Cayley’s notation slightly to be consistent with current notation, other than his practice of not using parentheses.

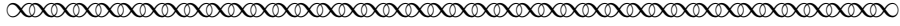
<sup>34</sup>A caustic is a curve related to the reflection (or refraction) of light off a surface in the study of optics. Cayley did not say more about this example in his 1854 group theory paper, but did describe it in considerable detail in his paper “On a property of the Caustic by refraction of a Circle.” Interestingly, these two papers were submitted for publication in the journal *Philosophical Magazine* on the same day, and some scholars (e.g., [Chakraborty and Chowdhury, 2005]) contend that it was Cayley’s discovery of this second concrete example of a non-abelian group of order 6 which inspired him to generalize the abstract group concept from that of a permutation group.

### APPENDIX III: Camille Jordan, and equivalence modulo a normal subgroup

In Section 5 of his discussion of the quotient group concept, Hölder stated:



The explanations of the previous paragraphs can also be expressed as follows: One could call two elements from the entire group  $G$  *equivalent*, if they can be conveyed into each other through multiplication by an element of the distinguished (normal) subgroup  $H$ . Due to the interchangeability of the group  $H$  with the elements of the entire group, one need not distinguish in this definition between right and left multiplication. For the same reason, it follows that multiplying equivalents by equivalents yields equivalents. Thus if one partitions the elements of the entire group into classes, such that equivalent elements sit in the same class, and inequivalent elements in different classes, then one obtains a composition of the classes, for which the group property holds.



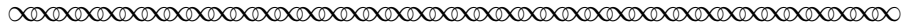
As noted earlier in this project, Hölder remarked no further on these claims, but simply took the notion of equivalency modulo a (normal) subgroup as well-known at the time. Indeed, mathematicians in his era had been working implicitly with this notion for years within the context of permutation groups, and the algebraist Camille Jordan<sup>35</sup> (1838–1922) had even explicitly written about it within that context in his paper “Sur la limite de transitivité des groups non alternés (On the limits of transitivity in non-alternating groups)” [Jordan, 1872–1873]. In this appendix, we explore the concept of an equivalence relation in general, as well as the particular equivalency relation on a group that is defined by a (normal) subgroup through excerpts from this paper.

We begin with an excerpt from Part I of Jordan’s paper,<sup>36</sup> in which he outlined his motivation for explicitly introducing equivalency notation into the study of permutation groups.

---

<sup>35</sup>Camille Jordan’s family included famous painters, politicians and scientists. Jordan himself entered the École Polytechnique to study mathematics in 1855. He completed a two-part doctoral thesis which addressed topics in algebra and integral equations in 1861. Afterwards, he worked for a time as an engineer before stepping into a professorial appointment at the École Polytechnique in 1876, one of several that he held throughout his lifetime. As a research mathematician, Jordan contributed to essentially every mathematical field studied at the time. He work was particularly influential in the theory of permutation groups, for which he proved a version of the theorem which came to be known as the Jordan-Hölder theorem. He also contributed significantly to efforts to classify all groups of finite order. Jordan’s comprehensive text *Traité des substitutions et des équations algébriques*, published in 1870, was awarded the Poncelet Prize by the French Académie des Sciences and became the standard reference in the study of group theory for years to come. He is also remembered today by analysts and topologists for his work on the Jordan curve theorem, which states that a simply closed curve divides a plane into exactly two regions; his other contributions to analysis include a generalisation of the criteria for the convergence of a Fourier series. In 1912, Jordan retired from his various academic positions, including editor of the important *Journal de Mathématiques Pures et Appliquées* which he has assumed in 1855. Sadly, his final years saw three of his six sons killed in World War I. Jordan himself passed away in Paris in 1922.

<sup>36</sup>All translations into English from Jordan’s paper are due to the project author.



Around the year 1845, the era when the work of M. Bertrand drew Cauchy's attention to the theory of substitutions [permutations], that great mathematician undertook an extensive series of research into that subject, the results of which are found in the *Comptes Rendus*.

The principal theorem that he obtained is the following

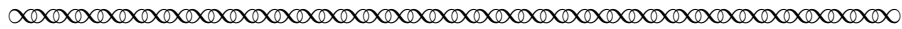
*Every group with order divisible by a prime number  $p$  contains an element<sup>37</sup> of order  $p$ .*

The importance of this proposition is manifest, and one may be surprised that it has given rise, thus far, to almost no application. But Cauchy's theorem has at last been completed and generalized, in the most happy fashion, by the Norwegian, M. Sylow.<sup>38</sup>

...

By its simplicity, its clarity and its generality, [M. Sylow's] proposition<sup>39</sup> surely merits to be considered fundamental; and we have not doubt that it will lead to important consequences.

In this paper, we give a first application [of Mr. Sylow's theorem] to the study of the limit of transitivity for permutation groups.




---

<sup>37</sup>In keeping with the more general context of this project, we have again use the word 'element' in place of Jordan's term 'substitution' when he was writing of individual elements of a permutation group. Although Jordan did work within the context of permutation groups himself, the theorems we cite in this project were soon recognized as valid for any arbitrary group.

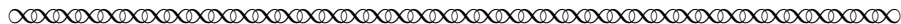
<sup>38</sup>After completing his studies at Christiania University, the Norwegian mathematician Peter Ludwig Mejdell Sylow (1832–1918) taught mathematics at the high school level from 1858–1898. Throughout this time, he continued to study, and eventually contribute to, advanced mathematical topics on his own. Sylow found the papers on the solvability of algebraic equations by radicals that were written earlier in the nineteenth century by his fellow countryman Niels Abel (1802–1829) to be of particular interest. The theory of equations was thus one of the topics that Sylow studied while visiting Berlin and Paris on a travel scholarship in 1861. Upon his return to Norway in 1862, Sylow delivered a series of lectures on Galois theory while serving as a substitute instructor at Christiania University. It was during these lectures that he posed the question that led to the important "Sylow Theorem" for which he remains justifiably famous today. His proof of this profound result, which he is believed to have completed as early as September 1870, was published in the 10-page paper *Théorèmes sur les groupes de substitutions* in 1872. Sylow's earlier 1862 lectures at Christiania University were also successful in providing a fundamental appreciation of Galois theory to those who attended them, including a young Sophus Lie (1842–1899) who went on to become a renowned mathematician in his own right. In 1894, the University of Copenhagen awarded Sylow an honorary doctorate, thereby allowing him to spend the final 20 years of his life teaching as a university professor in a special chair which Lie arranged to have created especially for Sylow at Christiania University.

<sup>39</sup>The proposition being praised by Jordan in this excerpt is a three-part theorem giving detailed information about the number of subgroups of a fixed order that a given finite group necessarily contains. As Jordan noted, Cauchy had already proved that a group whose order is divisible by a prime  $p$  has an element of order  $p$ , which in turn implies that the group contains a (cyclic) subgroup of order  $p$ . Sylow's generalization of this basic result can be stated as follows:

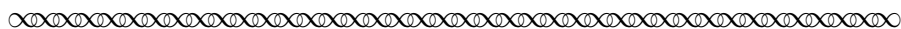
**Sylow's Theorem** If  $p^n$  is the largest power of the prime  $p$  to divide the order of a group  $G$ , then

1.  $G$  has subgroups of order  $p^n$ .
2.  $G$  has  $1 + kp$  such subgroups (which are today called  $p$ -Sylow subgroups).
3. Any two such subgroups are conjugate; that is, if  $H, K$  are subgroups of  $G$  of order  $p^n$ , then there exists  $x \in G$  such that  $K = x^{-1}Hx$ .

After providing, in Part I of his paper, the promised first application of Sylow's celebrated theorem, Jordan began Part II of his paper as follows:



We will now deduce from these same principles a new theorem, more extensive than any previous results. But to do so, it will be good to resume the proof of an auxiliary proposition that we have established elsewhere in its essentials (*Traité des substitutions*, 595), but by indirect means and under a statement that will not be convenient in the current question. The developments into which we will enter, and the definitions on which they are based seem, moreover, likely to considerably simplify the demonstration of several important propositions.



In the remainder of this appendix, we take a look at the definitions to which Jordan referred in this last excerpt, and how those definitions relate both to the concept of a quotient group and the current definition of an equivalence relationship. First, let us recall that current definition:

### Definition and Notation

Let  $S$  be a set and  $\mathcal{R}$  a (binary) relationship on  $S$ ; that is,  $\mathcal{R} \subseteq \{(x, y) \mid x, y \in S\}$ .

Given  $x, y \in S$ , the notation  $x\mathcal{R}y$  denotes that  $(x, y) \in \mathcal{R}$ .

$\mathcal{R}$  is an **equivalence relationship** on  $S$  if and only if the following three properties hold;

- (1)  $\mathcal{R}$  is **reflexive**:  $(\forall x \in S)(x\mathcal{R}x)$
- (2)  $\mathcal{R}$  is **symmetric**:  $(\forall x, y \in S)(x\mathcal{R}y \Rightarrow y\mathcal{R}x)$
- (3)  $\mathcal{R}$  is **transitive**:  $(\forall x, y, z \in S)(x\mathcal{R}y \wedge y\mathcal{R}z \Rightarrow x\mathcal{R}z)$

Here are two standard examples of equivalence relationships with which you are already familiar:

- Equality ( $=$ ) on any set of objects  $S$ ; and
- Equivalence on the set of fractions  $S = \{\frac{m}{n} \mid m, n \in \mathbb{Z}^+\}$ , where the fractions  $\frac{m}{n}, \frac{k}{l} \in S$  are said to be equivalent if and only if they both reduce to the same lowest term fraction  $\frac{a}{b} \in S$ .<sup>40</sup>

---

<sup>40</sup>The proof of transitivity under this definition of fraction equivalence is straightforward only if we know that all fractions reduce to a unique lowest-term fraction. For this purpose of this project, in which fraction equivalence is mentioned solely as a reminder of a familiar instance of an equivalence relationship, the reader may simply assume uniqueness of lowest-term representations for fractions without proof. This uniqueness assertion is itself a consequence of the uniqueness of prime factorization in the set of natural numbers; in fact, these two uniqueness theorems turn out to be equivalent! For more about this surprising and deep theorem, see David Pongelley's article *Quick, Does 23/67 Equal 33/97? A Mathematician's Secret from Euclid to Today* [Pongelley, 2013].



The first of these (equality) is the quintessential equivalence relationship, in that the three properties that all equivalence relationships are required to possess — reflexivity, symmetry and transitivity — were identified as the essential characteristics needed to capture the idea that any two equivalent elements seem ‘equal’ to each other in some way; in other words, all equivalent relations mimic equality in these three fundamental ways. Task III.1 examines another equivalence relationship with which you are likely also familiar, and compares it briefly to the relationship of equality (=).

**Task III.1** Given  $m \in \mathbb{Z}^+$  and  $x, y \in \mathbb{Z}$ , we say that  $x$  is congruent to  $y$  modulo  $m$  (denoted  $x \equiv y \pmod{m}$ ) if and only if  $m \mid (x - y)$ .

- (a) Verify that congruence modulo  $m$  on the set of integers satisfies the definition of an equivalence relationship.
- (b) For the sake of specificity, let  $m = 4$  and consider the relationship of integer congruence modulo 4.
  - (i) Find the set  $S_0$  of all  $x \in \mathbb{Z}$  such that  $x \equiv 0 \pmod{4}$ .  
 Given  $x, y \in S_0$ , what do you notice about the relationship between  $x$  and  $y$ ?  
 How else might you describe the elements of this set?
  - (ii) Find the set  $S_1$  of all  $x \in \mathbb{Z}$  such that  $x \equiv 1 \pmod{4}$ .  
 Given  $x, y \in S_1$ , what do you notice about the relationship between  $x$  and  $y$ ?  
 How else might you describe the elements of this set?
  - (iii) For a given  $r \in \mathbb{Z}$ , the set  $S_r = \{x \in \mathbb{Z} \mid x \equiv r \pmod{4}\}$  is called the *equivalence class of  $r$  modulo 4*. In parts (i) and (ii), you found two of the equivalence classes for the relationship of integer congruence modulo 4. Find all other distinct equivalence classes for this relationship, and justify your answer.
- (c) For a general equivalence relationship  $\mathcal{R}$  on a set  $S$ , the equivalence class of an element  $a \in S$  is defined as the set  $S_a = \{b \in S \mid a\mathcal{R}b\}$ . For the relationship of equality (=) on  $\mathbb{Z}$ , how many elements are in each equivalence class, and why?

In the following excerpt from [Jordan, 1872–1873], notice that he used the phrase “ordinary congruences” to refer to integer modular congruences<sup>41</sup> such as the one you examined in the preceding

---

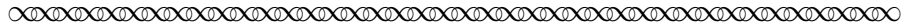
<sup>41</sup>The theory of integer congruences was first systematically developed by the celebrated mathematician Carl Friedrich Gauss (1777–1855), who also introduced the notation ‘ $x \equiv y \pmod{m}$ .’ Gauss was interested in solving number theoretic equations of the form  $x^m \equiv p \pmod{q}$ , where  $p$  and  $q$  are odd primes and  $x, m \in \mathbb{Z}^+$ . An especially famous result of this type is the *quadratic reciprocity law* which describes a relation between the solvability of the equations  $x^2 \equiv p \pmod{q}$  and  $x^2 \equiv q \pmod{p}$  for two different odd primes  $p, q$ . This difficult and beautiful result was first proven by Gauss in his important 1801 treatise on number theory, *Disquisitiones Arithmeticae*, where he stated the quadratic reciprocity law for primes  $p, q$  as follows:

If  $q \equiv 1 \pmod{4}$ , then  $x^2 \equiv p \pmod{q}$  is solvable if and only if  $x^2 \equiv q \pmod{p}$  is solvable.

If  $q \equiv 3 \pmod{4}$ , then  $x^2 \equiv p \pmod{q}$  is solvable if and only if  $x^2 \equiv -q \pmod{p}$  is solvable.

Gauss also looked for reciprocity laws for higher powers, eventually formulating a law for the ‘biquadratic’ case [ $x^4 \equiv p \pmod{q}$ ] by introducing a new set of ‘integers’ known as the complex (or Gaussian) integers.

task. Also note that, where we have used the word ‘subgroup’ below, Jordan himself instead used the word ‘group.’ Given the context in which he was working, Jordan’s use of the word ‘group’ always referred to a group of permutations; in other words, to a subgroup of  $S_n$  for some  $n \in \mathbb{Z}^+$ . Although we have instead used the word ‘subgroup’ (in keeping with the more general context of this project), it will be helpful in completing some of the tasks below to keep in mind that Jordan himself always meant a group of permutations.



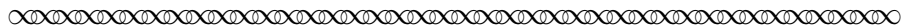
**7. Definitions.** — Two elements  $s$  and  $t$ , commutable with the subgroup  $H$ , are said to be *congruent module the subgroup  $H$*  if there is an equality of the form

$$s = th,$$

$h$  being an element of  $H$ .

One can express this relation by a formula analogous to that of ordinary congruences:

$$s \equiv t \pmod{H}.$$



Let’s pause here to examine Jordan’s definition.

### Task III.2

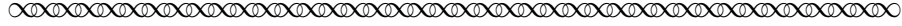
Assume  $G$  is a group and  $H$  is a subgroup of  $G$ .

- (a) What does Jordan mean by the expression “[the] elements  $s$  and  $t$  [are] commutable with the subgroup  $H$ ”? How would Hölder refer to a subgroup  $H$  with which all elements of the group  $G$  are commutable?
- (b) Prove that the definition given by Jordan in the preceding excerpt satisfies the definition of an equivalence relationship. Explain why it is *not* necessary to assume that the  $s, t$  are commutable with  $H$  in order to carry out this verification.

### Task III.3

Let  $G = \mathbb{Z}$  and  $H = \langle 4 \rangle$ . Find the equivalence classes of  $G$  for the congruence relationship modulo  $H$ . Compare these to what you found in Task III.1.

As you continue now with your reading of Jordan, pay attention to the types of objects that he is multiplying.



One can multiply two congruences member by member. In fact [from]

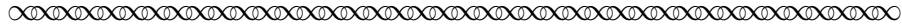
$$\begin{aligned} s &\equiv t \pmod{H} = th \\ s' &\equiv t' \pmod{H} = t'h' \end{aligned} ,$$

one will have

$$ss' = tht'h' = tt't'^{-1}ht'h',$$

and since  $t'^{-1}ht'$  is an element of  $H$ , by assumption,

$$ss' \equiv tt' \pmod{H}$$



#### Task III.4

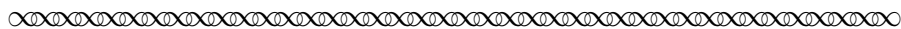
Describe the type of objects that Jordan was multiplying here. How are these related to the types of objects that Hölder was multiplying in his description of the quotient group in the excerpt on pages 10–1 of this project?

#### Task III.5

Re-read Jordan's proof that  $ss' \equiv tt'$ , provided  $s \equiv t$ , and  $s' \equiv t'$ .

What assumption specifically did Jordan make in Section 7 of his paper that allowed him to conclude that  $t'^{-1}ht'$  is an element of  $H$ ? Why is it important to know that  $t'^{-1}ht'$  is an element of  $H$ ?

As you read the final excerpt that we will consider from Jordan's paper, pay attention to how his notion of the group that Jordan denoted by ' $\frac{G}{H}$ ' compares to the concept that Hölder formally christened as a quotient group.

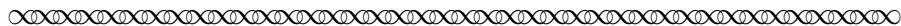


We will say that a [set] of elements  $s_1, s_2, \dots$  (all commutable with the same subgroup  $H$ ) forms a *group modulus*  $H$ , if there is for all values of  $\alpha$  and  $\beta$  a relationship of the form

$$s_\alpha s_\beta \equiv s_\gamma \pmod{H}$$

The *order* of this group will be the number of distinct elements, incongruent under the modulus  $H$ , that it contains.

Let  $G$  be the group derived from the elements  $s_1, s_2, \dots$ , where these are combined between them in the usual manner. We designate by  $\frac{G}{H}$  the group formed by these same elements under the modulus  $H$ . It is straightforward to see that the order of  $G$  is equal to the product of the order  $O$  of  $\frac{G}{H}$  by the order  $\Omega$  of the group  $I$  formed by the elements that are common to  $G$  and  $H$ .



### Task III.6

What is the name we give today to the group property that Jordan described by “there is for all values of  $\alpha$  and  $\beta$  a relationship of the form  $s_\alpha s_\beta \equiv s_\gamma \pmod{H}$ ”? Why is it sufficient for him to require that the set  $H = \{s_1, s_2, \dots\}$  satisfies this property in order to conclude that the set  $H$  forms a group?

### Task III.7

Describe carefully the type of objects in the set that Jordan denoted  $\frac{G}{H}$ . Notice that these are *not* cosets, as was the case for the objects that Hölder included in the quotient group  $G/H$ . How are the elements of Jordan’s group  $\frac{G}{H}$  related to those of Hölder’s quotient group  $G/H$ ?

### Task III.8

Why do you think Jordan brought in the group “ $I$  formed the elements that are common to  $G$  and  $H$ ” in his statement concerning the order of the group  $G$ ? Why was it not necessary for Hölder mention this group  $I$  in his discussion of the quotient group  $G/H$ ?

Jordan went on in his paper to discuss properties of isomorphic groups of the form  $\frac{G}{H}$ ,  $\frac{G'}{H'}$ , and to relate these back to the idea of the factors of composition that Hölder discussed in Section 3 of this project. As these ideas go beyond the scope of this project, we leave off our reading of Jordan’s paper at this point. To bring this appendix to closure, we instead look at another important property of equivalence relationships, again relating it back to the specific equivalence relationship of congruence modulo a subgroup  $H$  in the two tasks that follow the general definition given on the next page.

### Definition

Given a set  $S$ , let  $P_\alpha$  be a non-empty subset of  $S$  for each  $\alpha \in I$ , where  $I$  is an indexing set. The collection  $\mathcal{P} = \{P_\alpha\}_{\alpha \in I}$  is a **partition** of  $S$  if and only if every element of  $S$  appears in one and only one  $P_\alpha \in \mathcal{P}$ . That is,  $\mathcal{P} = \{P_\alpha\}_{\alpha \in I}$  is a partition of  $S$  if and only if the following conditions hold:

1.  $S = \bigcup_{\alpha \in I} P_\alpha$ .
2. The subsets  $P_\alpha$  are mutually disjoint: given  $\alpha, \beta \in I$  with  $\alpha \neq \beta$ , then  $P_\alpha \cap P_\beta = \emptyset$ .

### Task III.9

Let  $G$  be a group and  $H$  a subgroup of  $G$ . In Task III.2, you proved that the relationship

$$s \equiv t \pmod{H} \text{ if and only if } s \in tH$$

defines an equivalence relationship on  $G$ , even in the case where  $H$  is not normal in  $G$ . Let  $\mathcal{P}$  be the collection of all (left) cosets of  $H$ ; that is,  $\mathcal{P} = \{aH \mid a \in G\}$ .

- (a) Prove that  $\mathcal{P}$  is also the set of equivalence classes modulo  $H$ .

That is, prove that for all  $a, b \in G$ , we have  $aH = bH$  if and only if  $a \equiv b \pmod{H}$ .

Notice that this means  $aH = bH$  if and only if  $a \in bH$ , so that every element of the coset  $bH$  gives us another ‘name’ for that coset, and only those elements do so. This notion of having multiple names for one object is analagous to what happens with a set of equivalent fractions (e.g.,  $\frac{6}{8}$  and all other fraction equivalents of  $\frac{3}{4}$  serve as names for “the same fraction”).

- (b) Prove that the elements of  $\mathcal{P}$  are mutually disjoint.

That is, prove that for all  $a, b \in G$ , we have  $aH \neq bH$  if and only if  $aH \cap bH = \emptyset$ .

(Note that the contrapositive of this states:  $aH = bH$  if and only if  $aH \cap bH \neq \emptyset$ .)

- (c) Now complete the proof that  $\mathcal{P}$  is a partition of  $G$  by explaining why  $G = \bigcup_{a \in G} aH$ .

**Task III.10** This task generalizes Task III.9 to an arbitrary equivalence relationship.

- (a) Let  $S$  be a set and  $\mathcal{R}$  an equivalence relationship on  $S$ .

Let  $\mathcal{P}$  be the set of equivalence classes of  $\mathcal{R}$ .

Prove that  $\mathcal{P}$  defines a partition of  $S$ .

- (b) Now let  $S$  be a set and  $\mathcal{P} = \{P_\alpha\}_{\alpha \in I}$  be a partition of  $S$ , where  $I$  is an indexing set. Define the relationship  $\mathcal{R}$  on  $S$  as follows:

$$s \mathcal{R} t \text{ if and only if } (\exists \alpha \in I)(s \in P_\alpha \wedge t \in P_\alpha)$$

Prove that  $\mathcal{R}$  is an equivalence relationship on  $S$ .

# Notes to Instructors

## PSP Content: Topics and Goals

Today's undergraduate students are typically introduced to quotient groups only after meeting the concepts of equivalence, normal subgroups and cosets. Not surprisingly, the historical record reveals a different course of development. Although quotient groups implicitly appeared in Galois' work on algebraic solvability in the 1830's, 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 [42, 41]. Thus, when Hölder gave what is now considered to be the first "modern" definition of quotient groups in 1889, he was able to treat the concept as neither new nor difficult [38]. This Primary Source Project (PSP) 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.

## Student Prerequisites

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 is 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 in Section 6 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. Some tasks in Section 4 of the project also include optional question phrasing for students who have previously studied group isomorphisms (which some textbooks introduce prior to discussing homomorphisms), but again in a way that does not require prior study of group isomorphisms. For students who have studied group isomorphisms prior to this project, certain parts of Task 29 in Section 6 could be omitted; these are identified as optional in that task.

## PSP Design, and Task Commentary

The full PSP is divided into six core sections of differing length, plus a project introduction and three optional appendices. A sample implementation schedule is included later in these Notes. The following description of the content of each section should assist instructors in determining how best to adapt that recommended schedule to their own course goals and students' needs. The estimated number of class periods (based on a class length of 55 minutes) is given for each section. The actual number of class periods spent on each section naturally depends on the instructor's goals and on how the PSP is actually implemented with students. Estimates on the high end of the range assume most PSP work is completed by students working in small groups during class time.

- Introduction (0 days, out-of-class reading only)

This section includes some historical background related to quotient groups, brief biographical information about Hölder, and an overview of the project design.

- Section 1: Hölder's Definition of a Group (0.5 class days)

This short section briefly examines Hölder's definition of a group, and prompts students to compare it to the usual definition found in today's textbooks. Hölder's definition assumed only closure, associativity and left- and right-cancellation. Since he worked strictly with finite groups, Hölder did not need to explicitly assume the existence of an identity or of inverses. He did, however, remark that both properties are implied by his definition, and Task 2 asks students to verify this for finite groups. Since students will have studied the definition of a group prior to starting this project, a brief whole class discussion of this section should suffice, with Task 2 itself either skipped altogether, or assigned solely as homework.

- Section 2: A Special Type of Subgroup (1–1.5 class days)

This section focuses on Hölder's definition of a normal (or distinguished) subgroup, together with alternate definitions and standard tests (e.g., only two left-cosets) for normality. The tasks in this section prompt students to examine these different definitions within the context of specific examples of normal subgroups. Tasks 3 and 4 are recommended as advance preparation work prior to the first class discussion of this section. The remainder of the tasks in this section are sufficient in number to allow for some to be completed in class via small group work and others to be assigned for individual write-ups as homework. These include a number of proof exercises that instructors could choose from for presentation as class examples, after first asking student to draft their own proof as advance class preparation prior to that presentation.

- Section 3: From “Factors of Composition” to “Quotient Groups” (0.5–1 days)

The purpose of this short section is to provide context for why Hölder himself was motivated to define the concept of a quotient group; namely, to generalize Jordan's previous result on group “factors of composition” to a more abstract setting. The outcome of Hölder's effort is today's Jordan-Hölder Theorem. Although this theorem is a deep result itself, Hölder's discussion of it in the this part of his paper was quite elementary. There are only two tasks in this section, which instructors should encourage students not to overcomplicate! Task 9 examines the definition and examples of a *maximal normal subgroup*, and is well-suited for completion as advance preparation prior to class discussion. Task 10 prompts students to compute the factors of composition for a specific group as a means to illustrate the content of Jordan's theorem, and is best-suited for completion in small groups during class.

- Section 4: Quotient Groups and Normal Subgroups (1–1.5 days)

This section begins with Hölder’s initial argument — cast within a concrete language that views ‘cosets’ simply as horizontal rows of a certain table — that a normal subgroup allows us multiply cosets of that subgroup in such a way that these new elements (i.e., cosets) will themselves form a group. His discussion of the role of normality in ensuring that the product of two cosets (i.e., rows of the table) is well-defined is examined through the project narrative, as well as several student tasks (Tasks 11–13). Other tasks in this section focus on basic properties of quotient group (Task 14) or on specific examples of coset and quotient group computations (Tasks 15–17). The groundwork accomplished in these specific examples is intended to set the stage for Hölder’s more abstract discussion of the concept of coset multiplication and the quotient group concept that appears in Section 5 of this project. As students first introduction to the notion of coset multiplication, these tasks are thus especially recommended for in-class completion via small group work. Task 18, which calls for students to re-write a proof from Section 1 in the more abstract language of cosets, is best-suited for individual write-up as a formal homework assignment.

- Section 5: The Importance of Being Normal (1–1.5 days)

This section continues with Hölder’s discussion of the quotient group as he moves from the concrete language of horizontal rows in a table to the more abstract language of “partitioning the group into classes of equivalent elements.” Tasks 20 and 21 ask students to examine what it means for coset multiplication to be well-defined from this perspective. Following a formal (re-)statement of the definition of quotient group and index (as part of the project narrative), the section closes with three tasks (22–24) that ask students to apply elementary group theory theorems to the quotient group itself. Instructors could choose to present one or more of these as a class example (after asking students to draft their own solution as advance preparation for class), and assign the rest for either in-class small group work or individual write-up as homework.

- Section 6: The Fundamental Homomorphism Theorem (2.5–3 days)

This section employs Hölder’s comments on homomorphisms as a launching board for a series of tasks that explore basic properties of homomorphisms (Tasks 26, 27, 29), as well as several concrete examples (Tasks 28, 30, 31, 32). This latter set of tasks are especially important for students to work through on their own or in small groups in order to set the stage for their recognition of the Fundamental Homomorphism Theorem (FHT) and related preliminary results. These preliminary results (Theorem 1 on page 23 and Theorem 2 on page 24) are examined in Tasks 33–35, with Task 34 again providing a specific example that is best-suited for small group exploration.

The pièce de resistance — of this section and the entire project — comes in Hölder’s statement of the Fundamental Homomorphism Theorem itself, which is then re-stated formally (in Theorem 3 on page 25), via a diagram (Figure 1 on page 25) and schematically (Task 36 on page 25). Task 41 leads students through a full formal proof of FHT, and can easily be completed by them individually (as advance preparation work or as homework). Four other tasks in this section (Tasks 37–40) prompt students to apply FHT either to specific groups or to proofs of related theorems. The section (and project) then closes with some brief comments from Hölder’s about “splitting the group into two factors” using a normal subgroup and the corresponding factor group, and two final tasks (Tasks 42–43) that explore how this idea can be used in practice. Instructors could choose to present one of the more theoretical tasks from this section (Tasks 37–40, 42–43) either in part or entirety as class examples (after asking students to draft their own solution as advance preparation for class), and assign the rest for either in-class small group work or individual write-up as homework.



- **Appendix I: Cauchy’s Proof of Lagrange’s Theorem for Permutation Groups (Optional, 1–1.5 days)**  
In his initial description of the quotient group defined by a normal subgroup (Section 4), Hölder remarked that the array scheme he was employing had already been used in Augustin Cauchy’s proof of Lagrange’s Theorem in the particular case of a permutation group. This appendix presents Cauchy’s original proof of that theorem and examines it within a particular example that illustrates the concept of cosets and equivalency modulo a subgroup, but without using this more abstract language. It is included with this project in part for the sake of completeness. However, instructors who wish to provide students with a more concrete introduction to Lagrange’s Theorem could use this appendix (or the full-length primary source project one which it is based, described in more detail later in these Notes) as students’ first introduction to that theorem and its proof. Completion of this Appendix, and especially Task I.2, could also be assigned as a substitute make-up assignment for students with missing course work, or as an extra credit assignment for interested students.
- **Appendix II: Cayley’s Classification of Groups of Small Order (Optional, 0.5–1 day)**  
This appendix features the conclusion of Cayley’s analysis of all groups of order 6, in which he established that there are only two such groups. The Cayley tables that he produced as part of this proof include a table for  $S_3$  in which the alternating subgroup  $A_3$  shows up in a fashion that beautifully and surprisingly reveals both quotient group  $S_3/A_3$  and the fact that  $S_3/A_3 \cong \mathbb{Z}_2$ ! This material is related to earlier tasks in the project (e.g., Task 8, 15, 18 & 28), and also provides students with the Cayley table for  $S_3$  which can be conveniently used to complete computations for Task 15 and Task 20.
- **Appendix III: Camille Jordan, and Equivalence Modulo a Normal Subgroup (Optional, 1–2 days)**  
This appendix uses excerpts from a work by Camille Jordan (1838–1922) to examine properties of the equivalence relationship of a group modulo a (normal) subgroup in more detail. Although Hölder referenced this relationship in the excerpt in Section 4 of this project, he simply took this relationship as well-known, due to the work which Jordan and others had done before him within the context of permutation groups. Instructors who wish students to be familiar with this more abstract approach to this material in more depth are thus advised to assign this Appendix in full or in part as a natural companion to Section 5 of the project. The material in this section is self-contained in the sense that it assumes no formal prior work with equivalence relationships on students’ part.

## 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; see pages 56 — 58 below for a sample guide. Reading Guides typically include “Classroom Preparation” exercises (drawn from the PSP Tasks) for students to complete prior to arriving in class; they may also include “Discussion Questions” that ask students only to read a given task and jot down some notes in preparation for class discussion. On occasion, tasks are also assigned as follow-up to a previous in-class discussion. In addition to supporting students’ advance preparation efforts, these guides provide helpful feedback to the instructor about individual and whole class understanding of the material. The author’s students receive credit for completion of each Reading Guide (with no penalty for errors in solutions).

L<sup>A</sup>T<sub>E</sub>Xcode of the entire PSP is available from the author by request to facilitate preparation of reading guides or ‘in-class task sheets’ based on tasks included in the project. The PSP itself can also be modified by instructors as desired to better suit their goals for the course.

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

### Day 1

- **Advance Preparation Work** – to be completed before class

Read pages 1–6 of the Introduction, Section 1 and Section 2, completing Tasks 1, 4 for class discussion along the way, per the sample Reading Guide on pages 56–58 below. Since Task 3 should be a straightforward application of the definition of subgroup by this point in the course, it could also be including on the Reading Guide, or simply assigned as later homework.

- **Class Work**

- Whole class and/or small group discussion of the following:
  - \* (Optional) Historical and mathematical ideas from the Introduction, if desired
  - \* Hölder’s definition of a group in Section 1, including answers to Task 1.
  - \* Assigned reading in Section 2, including comparison of answers to Task 4.
- Small group work on Task 5.
- Time permitting, the instructor could preview the definition in Task 6, or have students begin work on this task in small groups.

- **Homework** – to be due at a later date (e.g., one week after completion of the in-class work)

A complete formal write-up of some or all of Tasks 2, 3, and/or 5.

Note that parts of Task 2 are challenging, while Tasks 3 & 5 address essential course content.

### Day 2

- **Advance Preparation Work** – to be completed before class

- In Section 2, prepare notes for class discussion of Tasks 6 – 8.
- In Section 3, read page 8–9, completing Task 9 for class discussion along the way.

- **Class Work**

- Brief whole class discussion of terminology (i.e., ‘conjugates’) introduced in Task 6.
- Small group work on Tasks 6 & 8.
- Brief whole class discussion of Netto’s theorem in Task 8.
- Time permitting, small group discussion of answers to Task 9, and initial work on Task 10.

- **Homework** – to be due at a later date (e.g., one week after completion of the in-class work)

A complete formal write-up of some or all of Tasks 6–8.

Task 6 in particular addresses essential course content.

### Day 3

- **Advance Preparation Work** – to be completed before class  
In Section 4, read pages 9–12, completing Tasks 11, 12, 13 along the way.
- **Class Work**
  - Whole class discussion of the Hölder excerpt in the assigned reading.
  - Small group work on Tasks 14, 15, 16, & 17.
- **Homework** – to be due at a later date (e.g., one week after completion of the in-class work)  
A complete formal write-up of student work on Task 18.

### Day 4

- **Advance Preparation Work** – to be completed before class
  - As follow-up to Day 3 class work, read the remainder of Section 3 (pp. 14–15).
  - In Section 5, read pp. 15–18, completing Task 19 and 20 along the way.  
Also prepare notes for discussion of at least one of Task 22–24 (to be chosen by the instructor).
- **Class Work**
  - Summarizing whole class discussion of the definition of quotient group, emphasizing the importance of using a normal subgroup, possibly to include a review of answer to Task 20.
    - \* A review of the various methods for establishing normality encountered thus far in the project would also be useful at this point; these appear in Definition 1, Definition 1', Task and Task 18.
    - \* A presentation of the instructor's solution to the task selected from Tasks 22–24 for advance preparation by students is also recommended here as an example of how to apply elementary group properties to the quotient group.
  - Time permitting, small group work could begin on the rest of Tasks 22–24 (e.g., those not selected for instructor presentation as a class example).
- **Homework** – to be due at a later date (e.g., one week after completion of the in-class work)  
A complete formal write-up of student work on the rest of Tasks 22–24 (e.g., those not selected for instructor presentation as a class example).

### Optional Day on Appendix III

- **Advance Preparation Work** – to be completed before class  
In Appendix III, read pages 37–41, completing Tasks III.1, III.2 and III.3 for class discussion along the way.
- **Class Work**
  - Whole class or small group discussion of definitions in assigned reading, to include answers to Tasks III.2 and III.3.
  - In small groups (with whole class discussion as deemed appropriate):
    - \* Read page 42 and discuss Tasks III.4 and III.5.
    - \* Read page 43 and discuss Tasks III.6, III.7 and III.8.
- **Follow-up Work (to be due at start of next class period):** Complete reading of Appendix III (pp. 43–44), including any of Tasks III.4–III.8 that were not completed in class.
- **Homework** – to be due at a later date (e.g., one week after completion of the in-class work)  
A complete formal write-up of Tasks III.9 and III.10.

### Day 5

- **Advance Preparation Work** – to be completed before class  
In Section 6, read pages 19–20 and prepare notes for class discussion for Tasks 26, 27, 28, 29a.
- **Class Work**
  - Whole group discussion of the ideas in advance reading, to include Definition 3 and answers to some/all of Tasks 26, 27, 28, 29a.
  - Small group work on some selection of the following: Task 29b, 29c, 30, 31, 32
- **Homework** – to be due at a later date (e.g., one week after completion of the in-class work)  
A complete formal write-up of some or all of Task 29c, 29d and 29e.

## Day 6

- **Advance Preparation Work** – to be completed before class

In Section 6, read pages 22–23, preparing preliminary notes for class discussion on the following along the way: Tasks 33, 34a, 34b, 35

- **Class Work**

- Whole group discussion of Theorems 1 and 2 from the reading, to include requested proofs in Tasks 33 & 35 and answers to Tasks 34a & 34b.
- Small group work on Tasks 34c & 34d
- Time permitting, the instructor could use the specific examples in Tasks 31, 32 & 34 to preview the statement of the Fundamental Homomorphism Theorem

- **Homework** – to be due at a later date (e.g., one week after completion of the in-class work)

A complete formal write-up of student work on Tasks 33a & 34.

## Day 7

- **Advance Preparation Work** – to be completed before class

In Section 6, read pages 24–27, completing Tasks 36 & 41 and preliminary notes for class discussion on Task 37 & 42 along the way (and skipping all other tasks on these pages).

- **Class Work**

- Whole group discussion of the Fundamental Homomorphism Theorem, to include discussion of answers to Tasks 36 & 37.
- Whole class or small group discussion of Task 42
- Time permitting, whole class or small group discussion of one of the following (to be selected by instructor): Tasks 38, 39, 43

- **Homework** – to be due at a later date (e.g., one week after completion of the in-class work)

A complete formal write-up of some or all of the following (e.g., those not selected for instructor presentation as a class example): Tasks 39, 40, 42, 43.

## Connections to other Primary Source Projects (PSPs)

The author of the current project has developed and taught with the following additional PSPs addressing core topics from the standard curriculum of a junior-level abstract algebra course. Each of these projects has been successfully site-tested at several institutions as a replacement for a textbook, either for a portion of the course, or for the course in its entirety. Further information about structuring an entire Abstract Algebra course around PSPs in this collection is available from the author.

- *Abstract Awakenings in Group Theory:*  
*Early group theory in the works of Lagrange, Cauchy, and Cayley*<sup>42</sup>

The centerpiece of this extended PSP is the 1854 inaugural paper on abstract group, Arthur Cayley's *On the theory of groups, as depending on the symbolic equation  $\theta^n = 1$*  [Cayley, 1854]. In keeping with the historical record, and to provide concrete examples on which to base their abstraction of the group concept, Section 1 of the project begins with the material from Lagrange 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 which a more general theory of permutations and symmetric groups was developed independently of the theory of equations, and today's current notation for permutations was first introduced. Section 2 also includes Cauchy's statement and proof of Lagrange's Theorem for Symmetric Groups, both of which are easily adapted to the more general case of any finite group (as is illustrated in Appendix II of the current PSP, which contains this same material). 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.

---

<sup>42</sup>To obtain the most recent version of *Abstract Awakenings in Group Theory*, contact the author at [janet.barnett@csupueblo.edu](mailto:janet.barnett@csupueblo.edu), or visit [www.cs.nmsu.edu/historical-projects/projects.php](http://www.cs.nmsu.edu/historical-projects/projects.php) for an earlier version. Within that earlier version, all resolvent equation examples are instead presented as tasks for students to complete themselves. An alternative version of the PSP *The Roots of Early Group Theory in the Works of Lagrange* which adopts that more open-ended/inquiry-based approach is also available upon request from the author. This PSP was initially developed under NSF grant DUE-0715392l; additional testing has also been supported by funding from the TRIUMPHS NSF grant DUE-1523494.

- *The Roots of Early Group Theory in the Works of Lagrange*<sup>43</sup>

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

The design of project is based on the first section of the extended PSP *Abstract Awakenings in Group Theory*, the content of which is 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 and permutations / permutations groups in much, if any, detail.

- *Richard Dedekind and the Creation of an Ideal: Early Developments in Ring Theory*<sup>44</sup>

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 Dedekind devoted therein to motivating why ideals are of interest to mathematicians by way of examples from number theory that are readily accessible to students at this level. In this regard, unique prime factorization (and the failure thereof in certain integral domains) plays a central role. Other specific topics developed in the PSP include the following: rings, integral domains, fields, zero divisors, ideals, principal ideals, prime ideals, 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).

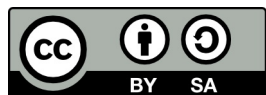
---

<sup>43</sup>To obtain the most recent version of *The Roots of Early Group Theory in the Works of Lagrange*, visit <http://webpages.ursinus.edu/nscoville/studentprojects.html>. An alternative version which 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 the author at [janet.barnett@csupueblo.edu](mailto:janet.barnett@csupueblo.edu). Development and testing of this PSP was supported by funding from the TRIUMPHS NSF grant DUE-1523494.

<sup>44</sup>To obtain the most recent version of *Richard Dedekind and the Creation of an Ideal: Early Developments in Ring Theory*, visit <http://webpages.ursinus.edu/nscoville/studentprojects.html>. Development and testing of this PSP was supported by funding from the TRIUMPHS NSF grant DUE-1523494.

## Acknowledgments

The development of this project has been partially supported 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 Program under Grant Number 1523494. Any opinions, findings, conclusions or recommendations expressed in this project are those of the author and do not necessarily represent the views of the National Science Foundation.



This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License (<https://creativecommons.org/licenses/by-sa/4.0/legalcode>). It allows re-distribution and re-use of a licensed work on the conditions that the creator is appropriately credited and that any derivative work is made available under “the same, similar or a compatible license”.

For more information about TRIUMPHS, visit <http://webpages.ursinus.edu/nscoville/TRIUMPHS.html>.



## SAMPLE READING GUIDE - For Day 1

Background Information: The goals of the reading and tasks assigned in this guide were to prepare students for a whole-class discussion of the definition and examples of a normal subgroup, and small group work on Task 6.

\*\*\*\*\*

### Reading Assignment *Otto Hölder's Formal Chrisening of the Quotient Group Concept* - pages 1–5

1. Read the Introduction, pp. 1 – 2. *Jot down any comments or questions you have here.*

2. In Section 1, read pages 2–3.

Then **complete Task 1** (page 2) in preparation for class discussion here:

**Task 1** Compare the definition of a group given by Hölder to the definition typically found in today's textbook. How are these definitions the same? How are they different?

3. SKIP TASK 2, and go on to read page 4 in Section 3.

**Write at least one question or comment about the mathematical ideas in the Hölder excerpt.**

4. **Write out a sketch for the proof requested in Task 3 (page 4).**

Do this on a separate sheet, and attach your work to this study guide.

*Questions or comments?*

*This reading guide is continued on the next page.*

5. Complete Task 4 from page 5.

**Task 4** Consider the specific group  $G = S_3$ , and denote the identity permutation by  $e$ .

(a) Let  $H = A_3 = \{ e, (1, 2, 3), (1, 3, 2) \}$ .

Find the transformed subgroup  $a^{-1}Ha$  for every element  $a \in S_3$ .

(A partial computation for  $a = (1, 2)$  is given below.)

$a$	$a^{-1}Ha$
$e$	
$(1, 2)$	$\{ (1, 2)e(1, 2), (1, 2)(1, 2, 3)(1, 2), (1, 2)(1, 3, 2)(1, 2) \} =$
$(1, 3)$	
$(2, 3)$	
$(1, 2, 3)$	
$(1, 3, 2)$	

What do you notice about the transformed subgroups in this case?

*This reading guide is continued on the next page.*

#### Task 4 - Continued

RECALL:  $G = S_3$ , where  $e$  denotes the identity permutation.

(b) Now let  $K = \langle (2, 3) \rangle = \{e, (2, 3)\}$ .

Find the transformed subgroup  $a^{-1}Ka$  for every element  $a \in S_3$ .

$a$	$a^{-1}Ka$
$e$	
$(1, 2)$	
$(1, 3)$	
$(2, 3)$	
$(1, 2, 3)$	
$(1, 3, 2)$	

What do you notice about the transformed subgroups in this case?

*This reading guide is continued on the next page.*

6. Read the rest of page 5, through to the top of page 6

- **Write down Definition 1 for a normal subgroup here.**

- **Write down Definition 1' for a normal subgroup here.**

- *Questions or comments?*

7. Also read — but do not complete! — Task 6.

- **What does it mean for a subgroup to be closed under conjugates?**

- **Write down the theorem which Task 6 asks us to prove.**

- *Questions or comments?*