Otto Hölder's Formal Christening of the Quotient Group Concept

Janet Heine Barnett*

April 20, 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 where he

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

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.[1]

I. Group theoretic section[2]

§ 1. Defining properties of groups

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

[1] 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:

[2] 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.

[3] 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 work '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

$$B, B_1, B_2, \ldots$$

form a "subgroup" of the entire group, then the elements "transformed with the help of the element A",

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

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.

$\boxed{\textbf{Task 4}}$ Consider the specific group[4] $G = S_3$, and denote the identity permutation by e.

(a) Let[5] $H = \langle(1,2,3)\rangle = \{\, e\,,\ (1,2,3)\,,\ (1,3,2)\,\}$.
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

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

[5] 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[6] (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*[7] *subgroup of G.*

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

(a) Explain why Netto could assert that $t, ts_2, ts_3, \ldots, ts_r$ are 'the remaining r elements of G' in his proof. Begin by clearly stating the assumptions that led him to this assertion.

(b) 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.)

(c) Explain why the equation $G^{-1}HG = H$ holds if and only if H is normal in G.

(d) Use Netto's Theorem to explain why[9] $A_n \triangleleft S_n$ for all $n \in \mathbb{Z}^+$.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

You can skip this section.

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.

Skip this task

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[10] $G = \mathbb{Z}_{12}$ 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

$$G, G', G'', ...J$$

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

$$n, n', n'', \ldots 1$$

elements respectively, then

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

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.[†]

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

[10] 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.

[†] 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.[11] 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.

Skip this task

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*[12]) are interpreted as identical. Here's an example.[‡]

[11]A polynomial is said to be algebraically solvable provided its roots can be obtained from its coefficients using only elementary arithmetic operations $(+, -, \times, \div)$ 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^{th} roots of unity.

[12]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.

[‡]Hö'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

$$B, B_1, B_2, \ldots$$

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

$$\begin{array}{cccc} B, & B_1, & B_2, & \ldots \\ S_1B, & S_1B_1, & S_1B_2, & \ldots \\ S_2B, & S_2B_1, & S_2B_2, & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ S_{n-1}B, & S_{n-1}B_1, & S_{n-1}B_2, & \ldots \end{array}$$

where the elements

$$S_1, S_2, ..., S_{n-1}$$

are appropriately chosen from the entire aggregate. This scheme is found already in Cauchy. Here's an example.§ 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 $S_1, S_2, ..., S_{n-1}$ are appropriately chosen from the entire aggregate' in the construction of the scheme (or array) found in Cauchy.[13].

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 $B, B_1, B_2, \ldots$ denote the elements of the subgroup H, while S_ν, S_μ, S_x denote elements of the group G in this continuation of the preceding excerpt.)

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

[13]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 μ, ν, ρ, σ signify four arbitrary indices, then it is always the case that[14]

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

where the index x depends only on μ and ν.

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 $B, B_1, B_2, \ldots$ denote the elements of the subgroup H, while S_ν, S_μ, S_x denote elements of the group G.)

(ii) Why was it important for Hölder to select *arbitrary* indices μ, ν, ρ, σ for this computation?

(iii) What did Hölder mean by the phrase 'the index x depends only on μ and ν'?

[14] 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, ...of the normal subgroup H for certain appropriately chosen elements $S_1, S_2, ..., S_{n-1}$ 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:

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

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 alluded 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.[15] 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:

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

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_ν' by 'the horizontal row corresponding to s_μ' 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:

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

[15] 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.

(a) 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 $(sH)[(uH)(yH)]$.

(b) Show that H is the identity element of G/H. *Hint:* $eH = H$.

(c) Given $sH \in G/H$, how should we define the inverse element $(sH)^{-1}$? Justify your answer.

Skip this task

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 $H = \{1\,,\,\alpha\,,\,\beta\,\}$.

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

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

(b) Complete the following Cayley table[16] for $G/H = \{\,H\,,\,\gamma H\,\}$.

	H	γH
H		
γH		

(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.]

Skip this task

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:

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

.

(a) Complete the following list of the five distinct cosets of G/H:

H	$=$	$\{\,0\,,\,5\,\}$	another name for this coset: $5 + H$
$1 + H$	$=$	$\{\,1\,,\,6\,\}$	another name for this coset: ______
$2 + H$	$=$		another name for this coset: ______
$3 + H$	$=$		another name for this coset: ______
$4 + H$	$=$		another name for this coset: ______

[16] 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.

Skip this task

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.]

Skip this task

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!).

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

(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[17] $(G : H)$. 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?)*

[17]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.

Skip this task

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*.[18] This isomorphism is called *merohedral*[19], because several elements of the first group correspond to one element of the second.

[18] 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.

[19] 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*[20] 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 <u>multiplying equivalents by equivalents yields equivalents</u>. 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:

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

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.

[20] 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.[21]

- $K = 1K = \{\,1\,,\,\gamma\,\} = \gamma K$
- $\alpha K = \{\,\alpha\,,\,\alpha\gamma\,\} = \{\,\alpha\,,\,\delta\,\} = \delta K$
- $\beta K =$ ____________________
- $K = K1 = \{\,1\,,\,\gamma\,\} = K\gamma$
- $K\alpha = \{\,\alpha\,,\,\gamma\alpha\,\} = \{\,\alpha\,,\,\epsilon\,\} =$ ______
- $K\beta =$ ______________________

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

(c) Compute the following 'coset products.'

- $\alpha K\beta K =$ _________________
- $\delta K\epsilon K =$ _________________

(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 $H \lhd G$, $s,t,u,v \in G$, $sH = tH$ 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:

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

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 $(st)H = (uv)H$.

[21] 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 $a \in G$, $\mathrm{ord}_{G/H}(aH)$ is a divisor of m.

(b) For all $a \in G$, $a^m \in H$.

Example of what a completed task looks like

Task 2 (a): We wish to show that an identity element in the group exists. We will employ our modern notation. Let G satisfy Holder's definition, and note that it is assumed that $|G| < \infty$. If $a \in G$, we can consider $a \cdot a = a^2$, $a \cdot a \cdot a = a^3$, and so forth. Eventually, one has $a^m = a^k$ for some $m, k > 0$ with $m \neq k$. If this does not occur, then each power of a is distinct. This contradicts the finiteness of G. **Finiteness is used here.**

Assume that $m > k$. From iterating condition 3), we have $a^{m-k}a = a$. We can see that a^{m-k} is the identity element. Indeed, for any $b \in G$, we have $ba^{m-k}a = ba$. Condition 3) implies $ba^{m-k} = b$. Grouping terms differently shows $aa^{m-k} = a$, so we can see that a^{m-k} is a two-sided identity. ✓