Investigating the Group Extension Problem

Dallas Anderson

June 15 2023

Abstract

In this paper we will talk about groups and basic group theory knowledge. We will mention how the Group Extension Problem relates to classifying all (finite) groups. Although the Group Extension Problem is still unsolved, we'll explore the cases where this has already been solved and show an example. Then, we'll look at some different ways to approach it in some other cases, from brute force to more elegant solutions.

1 Introduction

Out of all the objects in math, groups are one of the most fundamental. They show up everywhere ranging from physics to Galois theory to algebraic topology, quite a lot of places. They can describe symmetries of anything from a concrete object like a triangle, to an abstract object like a field or ring, or even another group! (Called an automorphism group.) But before we can use them we have to define them first.

Definition 1.1 A **group** is a set G equipped with a binary operation $\cdot : G \times G \to G$ (that is, if $g, h \in G$ then $g \cdot h \in G$) that satisfies a few special properties: Firstly, associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. Next, there's an element $e \in G$ such that

$$e \cdot x = x \cdot e = x,$$

and so that for every element $a \in G$ there's an element $a^{-1} \in G$ such that

$$a \cdot a^{-1} = a^{-1} \cdot a = e.$$

e is called the **identity element** and a^{-1} is called the **inverse** of a.

Example 1.2 Imagine all the ways of flipping around a triangle that leave it in the same position, that is, all the ways of shuffling the points on it (called a **permutation**) that leave them the same distance apart. Well, you could rotate it by certain amounts, reflect it by some different lines, things like that. The operation is **composition**, denoted $\circ$, where $g \circ h(x) = g(h(x))$. The outputs are indeed in the group (this is called closure) because if you apply one distance-preserving permutation after another, the distances are still preserved and the overall effect is still a permutation. Associativity is true because function composition is always associative:

$$(f \circ g) \circ h(x) = f(g(h(x))) = f \circ (g \circ h)(x).$$

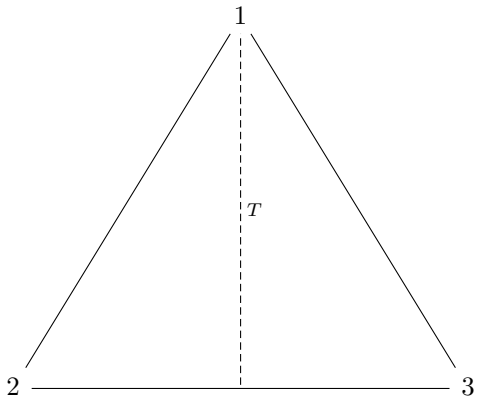
Next, we always count the do-nothing action e to be a permutation, and of course it preserves distances. We know that

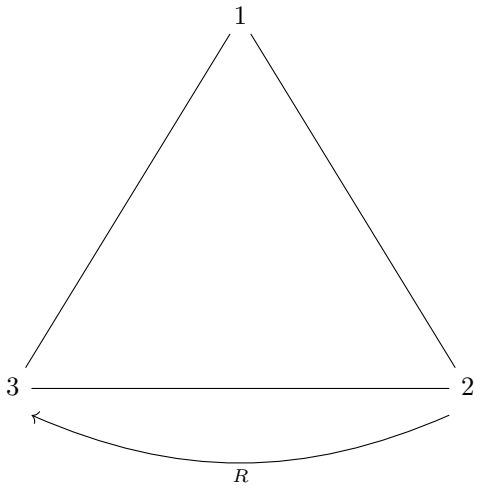
$$e \circ g = g \circ e = g$$

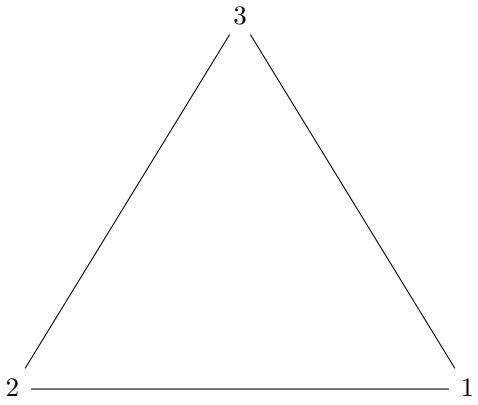
because e is doing nothing. For any distance-preserving permutation a, we can set a^{-1} to be the reverse of a, that is if $a(x) = y$ then $a^{-1}(y) = x$. We can see that a^{-1} is a distance-preserving permutation such that

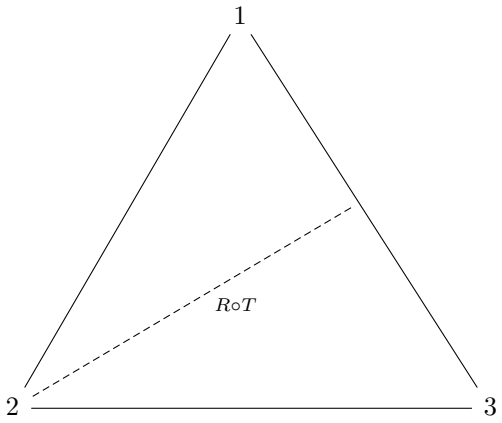
$$a \circ a^{-1} = a^{-1} \circ a = e.$$

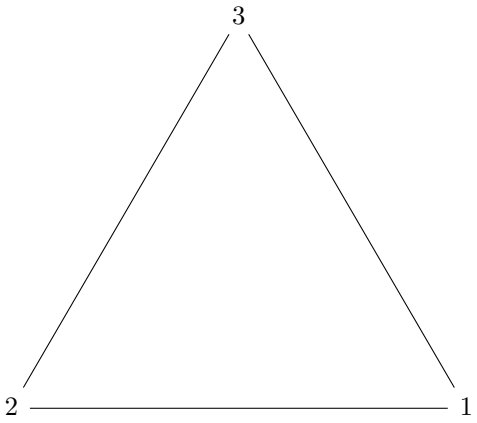
Here are some diagrams showing that if T is the vertical reflection and R is the 120° rotation counterclockwise, then $R \circ T$ is another reflection:











Because groups are so fundamental, it would be really useful to classify them. Similarly to how you can decompose integers via divisors into primes, you can also decompose groups via what are called normal subgroups into what are called simple groups.

Definition 1.3 If you have a group G and a subset H such that, under the same operation of G, H forms a group on its own, then we say H is a **subgroup** of G (denoted $H \leq G$). We say H is a **normal subgroup** of G, denoted $H \trianglelefteq G$, if for any $x \in H$ and $g \in G$, $g \cdot x \cdot g^{-1} \in H$. Taking gxg^{-1} for an element $x \in G$ is called **conjugating** by g.

Notice that if $g \cdot x = x \cdot g$ for all $x \in H$ and $g \in G$, then H is automatically a normal subgroup of G. Or, if $g \cdot h = h \cdot g$ for all $h, g \in G$, then all subgroups of G are normal.

Definition 1.4 We say a group G is **abelian** if $g \cdot h = h \cdot g$ for all $g, h \in G$.

Definition 1.5 Let $H \leq G$. Let $\sim$ be the equivalence relation so that $x \sim y$ if $y^{-1}x \in H$. We define the set G/H to be the collection of all equivalence classes under $\sim$. The elements of G/H are called **left cosets** of H, and the number of left cosets is called the **index** of H in G. We denote the equivalence class of an element g by $[g]$, or gH. If $H \trianglelefteq G$, then this set is a group under the operation $\cdot$ defined by $aH \cdot bH = abH$ (otherwise the operation is not well-defined). This group is called the **quotient group**.

Example 1.6 If you take the integers $\mathbb{Z}$ under addition, the odd numbers are not a subgroup because there exist two odd numbers that don't sum to an odd number (of course, they never sum to an odd number but existence is enough). Also, the nonnegative numbers are not a subgroup because although the sum of two of them is always nonnegative, the negative of a nonnegative number is not always nonnegative (only in the case of 0). However, if you check all the properties, you'll see that the even numbers (denoted $2\mathbb{Z}$) are a subgroup! So then $2\mathbb{Z} \trianglelefteq \mathbb{Z}$ since $\mathbb{Z}$ is abelian, and if you equivalence the integers by $x \sim y$ if $-y + x \in 2\mathbb{Z}$, then there are two equivalence classes: $2\mathbb{Z}$ itself, and the odd numbers, or $2\mathbb{Z} + 1$. We know that $0 + 0 = 0$, $0 + 1 = 1 + 0 = 1$, and $1 + 1 = 2 \sim 0$. If we label the even numbers e and the odd numbers o, we have that $e + e = o + o = e$ and $e + o = o + e = o$, and, checking the conditions, you can see that this is indeed another group (denoted $\mathbb{Z}/2\mathbb{Z}$)! Basically, $2\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$ are factor groups of $\mathbb{Z}$.

Example 1.7 As for our triangle example, again denoting the 120° rotation counterclockwise R and the vertical reflection T, it turns out all the symmetries are e, R, $R^2 = R \circ R$, T, $RT = R \circ T$, and $R^2T = R \circ R \circ T$. Now, e, R, and R^2 form a normal subgroup because $TRT^{-1} = TRT = R^2$, and vice versa, and we know that $TeT^{-1} = e$. It turns out that if you do this for anything, not just T, it still stays inside the subgroup, so this subgroup is indeed normal. If we take e and T, then while that forms a subgroup, it's not a normal one because $RTR^{-1} = R^2T$.

Notice how those subgroups have 2 and 3 elements respectively, both of which divide 6, the number of elements of the entire group. This is no coincidence:

Theorem 1.8 Let H be a subgroup of G. Then the number of elements in H, denoted $|H|$ divides $|G|$.

Remark. This theorem, called **Lagrange's theorem**, will be useful later.

Proof. Consider the set G/H. The notation aH suggests that $[a] = \{ah : h \in H\}$. This is in fact true. We know that $a^{-1}ah = h$, so $ah \sim a$ and $ah \in [a]$. But if $g \in [a]$ then $a^{-1}g = h$ for some $h \in H$, so $g = ah$. Next, you can check that if $ah = ah'$ then $h = h'$ (hint: $a^{-1}ah = h$), so $|H| = |aH|$. This shows that $|G|$ is just $|H|$ multiplied by the number of cosets of H, that is $|H||G/H| = |G|$. In particular, Lagrange's theorem holds true.□

Definition 1.9 The **order** of an element $g \in G$ is the smallest positive integer n such that $g^n = e$. If no such n exists, we say g has infinite order. We also define the order of a group to be its cardinality, or the number of elements it has.

So Lagrange's theorem says that the order of a subgroup divides the order of a group. It turns out that

the order of an element g is equivalent to the order of the subgroup $\langle g \rangle$, or the subgroup of powers of g (as we've seen with R and T; their orders are 3 and 2 respectively.) Thus Lagrange's theorem also tells us that the order of an element divides the order of a group.

Now we'll define simple groups.

Definition 1.10 A **simple** group is a group G containing non-identity elements such that the only normal subgroups of G are G itself and $\{e\}$.

The task of classifying (finite) simple groups was completed in 1981 with the efforts of hundreds of mathematicians (see [2]). What remains is to talk about how all (finite) groups decompose into simple groups. One thing that's nice is that, analogous to how prime factorizations of integers are unique, there's a theorem called the **Jordan-Hölder theorem** stating that decompositions of groups are unique too!

Theorem 1.11 Any two decompositions of any group G are the same up to reordering.

Now, to find the decomposition of a group, you just keep going down, keep factoring each new factor G into K and G/K for some (nontrivial) normal subgroup, until you get down to simple groups.

Definition 1.12 A **trivial subgroup** of a group G is a subgroup that's either G itself or just $\{e\}$. Note that these are both normal subgroups.

Here's a bit more precise way of decomposing:

Definition 1.13 A **maximal normal subgroup** N of G is a normal subgroup not equal to G such that if $N \leq K$ and $K \trianglelefteq G$ then $K = N$ or $K = G$. That is, there are no subgroups in between.

Lemma 1.14 A normal subgroup $N \trianglelefteq G$ is maximal iff G/N is simple.

Definition 1.15 Let G be a group. We call a series $A_1 \leq \cdots \leq A_n$ of subgroups of G such that $A_1 = \{e\}$ and $A_n = G$ a **composition series** for G if each term (other than A_n) is a maximal normal subgroup of the next. If you take A_{i+1}/A_i for each i you get a **decomposition** for G, and what the Jordan Hölder theorem really says is that any composition series of G gives the same simple group factors up to reordering.

Definition 1.16 Take any element e. The **trivial group** is the set $\{e\}$ with an operation defined by $e \cdot e = e$. Notice that this product is true if you take e to be the identity element of any group G, so the subgroup $\{e\}$ is always the trivial group.

Basically, the trivial group is analogous to 1 and simple groups are analogous to primes.

Example 1.17 In the case of the trivial group, the only decomposition series is $A_1 = \{e\}$ and nothing else. This leads to the empty factorization for the trivial group, which makes sense knowing that, in fact, $G/G \cong \{e\}$ and $G/\{e\} \cong G$. This is analogous to how anything to the power of 0 is 1.

Now, this does lead to problems with some infinite groups. For example, similarly to how 0 doesn't factor into primes because there's always a factor of 0, $\mathbb{Z}$ always has a factor of itself when you try to factor it. Of course, it's not literally contained inside itself, but it has a normal subgroup, infinitely many in fact, that are what's called isomorphic to it.

Definition 1.18 Let $\phi : G \to H$ be a function between two groups. We call ϕ a **homomorphism** if, for any $a, b, c \in G$ such that $a \cdot b = c$, $\phi(a) \cdot \phi(b) = \phi(c)$ as well. In other words, for any $a, b \in G$, $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$. We call ϕ a **bijection** if when $\phi(g) = \phi(h)$, $g = h$ (called **injectivity**) and for any $h \in H$, there's a $g \in G$ such that $\phi(g) = h$ (called **surjectivity**). Bijections are basically one-to-one correspondences. If ϕ is a bijection in addition to being a homomorphism, we call ϕ an **isomorphism**. Next, we say that G and H are **isomorphic**, denoted $G \cong H$, if there's an isomorphism between them. What isomorphic basically means is that two groups

are the same up to relabeling elements, and we only really care about groups to that extent.

Example 1.19 Let's try this for the integers and the even numbers. Take $\phi : \mathbb{Z} \to 2\mathbb{Z}$ so that $\phi(x) = 2x$. It's not hard to see that ϕ is a bijection, and since $2(a + b) = 2a + 2b$, we know that ϕ is an isomorphism. So $\mathbb{Z}$ factors into $\mathbb{Z}$ and another group with two elements. It turns out that all normal subgroups, even subgroups of $\mathbb{Z}$ are isomorphic to $\mathbb{Z}$ except $\{0\}$ whose quotient group is isomorphic to $\mathbb{Z}$. Thus, try as you might, you will indeed always have a factor isomorphic to $\mathbb{Z}$ when you factor it down.

Since we can't decompose some infinite groups, for the rest of the paper we'll focus more on finite groups.

Okay, so we have a way of uniquely factoring finite groups into simple groups. We know that prime factorizing integers has a lot of useful applications, but what about groups? One example is it's used in the proof of the unsolvability of the quintic. What does that mean? So, you know how there's a formula for the roots of a quadratic using the four basic operations along with radicals (specifically square roots) and, of course, the coefficients. Now, there's also a such formula for cubics, and even quartics! But mathematicians have really struggled to find a quintic formula and they still can't find one to this day! Why? Because it doesn't exist. Now, before we dive into this, we'll need a few definitions:

Definition 1.20 The **cyclic group** C_n is defined to be $\mathbb{Z}/n\mathbb{Z}$, where $n\mathbb{Z}$ is the normal subgroup of multiples of n.

Definition 1.21 We define a **symmetric group** S_n to be the group of permutations of n elements under composition.

Definition 1.22 A **transposition** is a permutation that switches two elements and leaves everything else where it is.

Definition 1.23 We define $A_n \leq S_n$, the **alternating group**, to be the subgroup of permutations that can be represented as a product (composition) of an even number of transpositions. Note that all permutations can be represented as a product of transpositions, and that the inverse of a product of transpositions is the product in reverse order, and so one can check that $A_n \trianglelefteq S_n$.

Theorem 1.24 There's no formula for the roots of a quintic polynomial using the four basic operations, radicals, and the coefficients.

Proof. It's not just that there's no formula, there's a specific quintic polynomial whose roots can't be expressed with the three things mentioned which has to do with the decomposition of S_5. To see this, first, it turns out that $S_n/A_n \cong C_2$ unless $n = 1$ (in which case $A_1 = S_1$ is the trivial group). If $n \geq 5$ then A_n is simple, and so the complete decomposition of S_n is A_n and C_2.

If the roots of our polynomial could be expressed with the three things mentioned, then that would mean the decomposition of S_5 would have to involve only cyclic groups C_p for p prime (we won't really get into why because that's a story for another paper). But A_5 is not of that form (or A_n for any $n \geq 5$), so there's no formula for quintics.□

This also shows there's no formula for n-degree polynomials when $n \geq 5$ because we could just multiply our quintic polynomial by x a bunch of times and that would only add to the roots.

The proof we've outlined leads to the notion of a solvable group.

Definition 1.25 A group G is called **solvable** if G decomposes into cyclic groups C_p for p prime (more generally if it can factor into abelian groups, e.g. now $\mathbb{Z}$ is solvable since it's already abelian).

Example 1.26 As we just saw, S_5 (or S_n for $n \geq 5$) is not solvable. However, S_1 through S_4 are solvable groups.

So that's one example of where this decomposition approach, and especially the Jordan-Hölder theorem, shows up.

2 The Group Extension Problem

One not-so-nice thing about group decomposition that's not true in our integer analogy is that different groups can have the same decomposition! For example, the direct product $C_2 \times C_2$, also denoted K_4, decomposes into C_2 and C_2. But C_4 also does, so those are two different groups with the same decomposition.

Definition 2.1 The **direct product** $G \times H$ of two groups G and H is the set of all pairs (g, h) where $g \in G$ and $h \in H$ under the operation

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot g_2, h_1 \cdot h_2).$$

Definition 2.2 Take any two groups K and Q. A group G such that $K \trianglelefteq G$ and $G/K \cong Q$ is called an **extension** of K by Q. More presicely, if there's a normal subgroup $K' \trianglelefteq G$ that's isomorphic to K, and if $G/K' \cong Q$, then we say G is an extension of K by Q.

Definition 2.3 The **Group Extension Problem**, formulated by O. Hölder, is the problem of, for given groups K and Q, finding all extensions of K by Q.

Now, it turns out that the case is a lot more complicated when K is nonabelian, so we'll start by focusing on the case where K is abelian.

Example 2.4 One case of a group extension G is a semidirect product. But before we define that, we'll need to define automorphism groups.

Definition 2.5 Let G be a group. An **automorphism** of G is an isomorphism from G to itself. We define the **automorphism group** $\mathrm{Aut}(G)$ to be the set of all automorphisms of G under the operation of composition.

Definition 2.6 We say that G is the **inner semidirect product** of subgroups K and Q, denoted $G = K \rtimes Q$, if K is normal, $K \cap Q = \{e\}$, and lastly $KQ = G$ (KQ denoting the subset of elements that can be expressed as an element of K times an element of Q).

Definition 2.7 If K and Q are groups and $\theta : Q \to K$ is a homomorphism, then the **outer semidirect product** $K \rtimes_\theta Q$ is defined so that the underlying set is again all ordered pairs (k, q) where $k \in K$ and $q \in Q$. Then, the operation on G is

$$(k_1, q_1) \cdot (k_2, q_2) = (k_1 \cdot \theta(q_1)[k_2], q_1 q_2).$$

It turns out that inner semidirect products and outer semidirect products are equivalent, so we just call them semidirect products.

It's checkable that if G is an inner semidirect product of K and Q, then $G/K \cong Q$, so this really is an extension of K by Q. In outer semidirect products, the isomorphic copy of K is $\{(k, e) : k \in K\}$, the isomorphic copy of Q is $\{(e, q) : q \in Q\}$, the identity is (e, e) and inverses are $(k, q)^{-1} = (\theta(q^{-1})[k^{-1}], q^{-1})$. Now, notice something about this. Assuming K is abelian, if you take any function $l : Q \to K$ that sends an element $q \in Q$ to (k, q) for some $k \in K$, then you have that

$$l(q)(k', e)l(q)^{-1} = (k, q)(k', e)(\theta(q^{-1})[k^{-1}], q^{-1}) = (k \cdot \theta(q)[k'], q) \cdot (\theta(q^{-1})[k^{-1}], q^{-1})$$

$$= (k \cdot \theta(q)[k'] \cdot \theta(q)[\theta(q^{-1})[k^{-1}]], qq^{-1}) = (k \cdot \theta(q)[k'] \cdot k^{-1}, e) = (\theta(q)[k'] \cdot kk^{-1}, e) = (\theta(q)[k'], e).$$

So, basically, conjugation by $l(q)$ is the same as applying $\theta(q)$.

Definition 2.8 If G is an extension of K by Q, we call a function $l : Q \to G$ a **transversal** if for any

coset $a \in G/K$, $l(a) \in a$. That is, l maps an element of Q into the corresponding coset.

This is one of many resources and background we'll need to develop in order to tackle the Group Extension Problem.

Definition 2.9 We call an ordered triple (Q, K, θ) **data** if Q is a group, K is an abelian group, and $\theta : Q \to \mathrm{Aut}(K)$ is a homomorphism. We say that a group G **realizes** this data if G is an extension of K by Q and, for every transversal $l : Q \to G$,

$$\theta_x(a) = \theta(x)[a] = l(x) + a - l(x).$$

(Note that we will be using additive notation for the operations in G and K, breaking convention. We'll still use multiplicative notation for Q, though.) We also denote $\theta_x(a)$ by xa.

As we just saw, the semidirect product realizes data (Q, K, θ). This actually generalizes.

Theorem 2.10 All extensions G of K by Q realize data (Q, K, θ) for some θ. Furthermore, θ is unique.

Proof. Take any transversal $l : Q \to G$, and let $\theta_x(a) = l(x) + a - l(x)$. Of course, θ can't be anything else, so this is the only possible solution. Next, we show θ is independent of the choice of transversal. For any two transversals l and l', we want to show that $l'(x) + a - l'(x) = l(x) + a - l(x)$ for any $a \in K$ and $x \in Q$. Since $l(x)$ and $l'(x)$ are both in the coset x, we know that $l'(x) - l(x) = k$ for some $k \in K$. Then,

$$l'(x) + a - l'(x) = l(x) + k + a - k - l(x) = l(x) + a + k - k - l(x) = l(x) + a - l(x).$$

Since conjugation is an automorphism, we know that at least $\theta : Q \to \mathrm{Aut}(K)$, and to see that θ is a homomorphism we use the same logic:

$$l(x) + l(y) + a - l(y) - l(x) = l(xy) + k' + a - k' - l(xy) = l(xy) + a + k' - k' - l(xy) = l(xy) + a - l(xy)$$

for a $k' \in K$. Thus $\theta : Q \to \mathrm{Aut}(K)$ is a homomorphism and G uniquely realizes the data.□

This means that we can narrow down the problem to finding all extensions realizing data (Q, K, θ), which is what we'll do.

Now, there are many extensions of K by Q other than the semidirect product.

Example 2.11 We know that C_4 is an extension of C_2 by C_2, but K_4 is the only semidirect product of them. If there's a transversal $l : Q \to G$ that's a homomorphism, that automatically means G is a semidirect product, so for the other cases l can never be a homomorphism. However, we saw above that $l(x) + l(y) = l(xy) + k'$ for some $k' \in K$. This principal leads us to consider the definition of a factor set.

Definition 2.12 If G realizes data (Q, K, θ) and $l : Q \to G$ is a transversal such that $l(1) = 0$, then the **factor set** $f : Q \times Q \to K$ (also called a **cocycle**) arising from the transversal l is defined so that $f(x, y) = l(x) + l(y) - l(xy)$. f essentially measures how 'far away' l is from being a homomorphism.

2.1 Group Cohomology

Here are the key properties that factor sets satisfy:

Theorem 2.1.13 For any group G realizing data (Q, K, θ) and any transversal l, the factor set f arising from l satisfies the following properties:

$$f(1, x) = f(y, 1) = 0,$$

and

$$f(x, y) + f(xy, z) = xf(y, z) + f(x, yz).$$

The latter is called the cocycle identity.

Proof. The first property is not too hard to check. As for the second property, we know that

$$f(x,y)+f(xy,z)+l(xyz) = f(x,y)+l(xy)+l(z) = (l(x)+l(y))+l(z) = l(x)+(l(y)+l(z)) = l(x)+f(y,z)+l(yz)$$
$$= xf(y,z) + l(x) + l(yz) = xf(y,z) + f(x,yz) + l(xyz).$$

The result follows from cancellation.□

What's really interesting, though, is that the converse is also true.

Theorem 2.1.14 For given data (Q, K, θ), any function $f : Q \times Q \to K$ satisfying the two above properties is a factor set arising from some transversal l of an extension G realizing the data.

Proof. We first construct G. The underlying set of G is, again, $K \times Q$ or (k, q) for $k \in K$ and $q \in Q$. The operation is

$$(k_1, q_1) + (k_2, q_2) = (k_1 + q_1k_2 + f(q_1, q_2), q_1q_2).$$

To start, let's check that this is a group.

The identity is $(0, 1)$. To see this, we compute:

$$(0, 1) + (k, q) = (0 + 1 \cdot k + f(1, q), 1 \cdot q) = (k, q).$$

Next,

$$(k, q) + (0, 1) = (k + q \cdot 0 + f(q, 1), 1 \cdot q) = (k, q).$$

Now, to see that the inverse of (k, q) is $(-q^{-1}k - q^{-1}f(q, q^{-1}), q^{-1})$, we know that

$$(k, q) + (-q^{-1}k - q^{-1}f(q, q^{-1}), q^{-1}) = (k + q(-q^{-1}k - q^{-1}f(q, q^{-1})) + f(q, q^{-1}), qq^{-1})$$
$$= (k - k - f(q, q^{-1}) + f(q, q^{-1}), 1) = (0, 1).$$

Next,

$$(-q^{-1}k-q^{-1}f(q,q^{-1}),q^{-1})+(k,q) = (-q^{-1}k-q^{-1}f(q,q^{-1})+q^{-1}k+f(q^{-1},q),q^{-1}q) = (-q^{-1}f(q,q^{-1})+f(q^{-1},q),1).$$

Uh-oh! It looks like we're stuck. After all, how can $-q^{-1}f(q, q^{-1}) + f(q^{-1}, q)$ simplify to 0? Well, if we plug in $x = q^{-1}$, $y = q$, and $z = q^{-1}$ to the cocycle identity, we get that

$$f(q^{-1}, q) = f(q^{-1}, q) + f(1, q^{-1}) = q^{-1}f(q, q^{-1}) + f(q^{-1}, 1) = q^{-1}f(q, q^{-1}).$$

Thus it does simplify to 0 after all, meaning $(-q^{-1}k - q^{-1}f(q, q^{-1}), q^{-1})$ is indeed the inverse of (k, q). Next, as for associativity, we have that

$$((k_1,q_1)+(k_2,q_2))+(k_3,q_3) = (k_1+q_1k_2+f(q_1,q_2),q_1q_2)+(k_3,q_3) = (k_1+q_1k_2+f(q_1,q_2)+q_1q_2k_3+f(q_1q_2,q_3),q_1q_2q_3).$$

For the other direction, we have that

$$(k_1,q_1)+((k_2,q_2),(k_3,q_3)) = (k_1,q_1)+(k_2+q_2k_3+f(q_2,q_3),q_2q_3) = (k_1+q_1(k_2+q_2k_3+f(q_2,q_3))+f(q_1,q_2q_3),q_1q_2q_3)$$
$$= (k_1 + q_1k_2 + q_1q_2k_3 + q_1f(q_2, q_3) + f(q_1, q_2q_3), q_1q_2q_3) = (k_1 + q_1k_2 + q_1q_2k_3 + f(q_1, q_2) + f(q_1q_2, q_3), q_1q_2q_3)$$
$$= (k_1 + q_1k_2 + f(q_1, q_2) + q_1q_2k_3 + f(q_1q_2, q_3), q_1q_2q_3).$$

Thus associativity holds. Closure is trivial, so G is a group. Identifying $k \in K$ with $(k, 1)$, you can check that this subgroup is isomorphic to K and that G quotient this subgroup is Q, so G really is an extension of K by Q.

Next, we need to check that G realizes data (Q, K, θ). Take any transversal l' of G. We want to show that

$qa = l(q) + a - l(q)$ for all $q \in Q$ and $a \in K$. That is, we want to show that $(qa, 1) = l(q) + (a, 1) - l(q)$. Firstly, denote $l(q) = (k, q)$. We have that

$$(k,q)+(a,1)-(k,q) = (k+qa,q)+(-q^{-1}k-q^{-1}f(q,q^{-1}),q^{-1}) = (k+qa+q(-q^{-1}k-q^{-1}f(q,q^{-1}))+f(q,q^{-1}),1) = (qa,1).$$

The last step is true since K is abelian.

Next, we define our transversal l so that $l(q) = (0, q)$. The factor set corresponding to l is $(f(x, y), 1)$, but as before we identify $(k, 1)$ with k so f is a factor set as desired.□

The group G we constructed, which we'll denote G_f, seems to generically represent f. I mean, the products are the same as in semidirect products except for that extra factor of f. Well, it turns out that these are all the extensions of K by Q realizing the data!

Theorem 2.1.15 Every extension G realizing data (Q, K, θ) is of the form G_f for some factor set $f : Q \times Q \to K$.

Proof. If you take any transversal l of any extension G (realizing the data), you can uniquely represent all elements of G as $k + l(q)$ for some $k \in K$ and $q \in Q$, so denote $k + l(q) = (k, q)$. Then

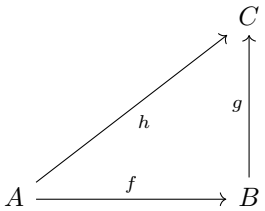
$$(k_1,q_1)+(k_2,q_2) = k_1+l(q_1)+k_2+l(q_2) = k_1+q_1k_2+l(q_1)+l(q_2) = k_1+q_1k_2+f(q_1,q_2)+q_1q_2 = (k_1+q_1k_2+f(q_1,q_2),q_1q_2).$$□

Pretty neat, isn't it?

We aren't quite done with our classification, though: How do we know that these extensions are all different? That is, how do we know that if $f \neq g$ then $G_f \neq G_g$? Well, that's actually not true, so how do we know when the extensions are the same? To find out, first we'll need a notion of equivalent extensions (and some definitions).

Definition 2.1.16 Consider any diagram of functions between sets. We say that the diagram **commutes** if, for any two fixed sets A and C on the map, the composition of any chain of functions along the diagram from A to C is always the same.

Example 2.1.17 The diagram below commutes iff $h = g \circ f$:



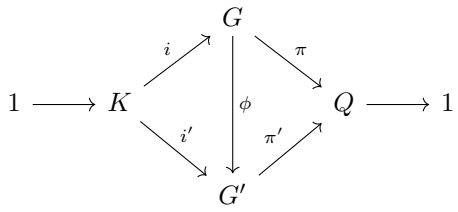
Definition 2.1.18 Take any homomorphism $\phi : G \to H$. We denote $\ker \phi$, called the **kernel** of ϕ to be the set of all $x \in G$ such that $\phi(x) = e$. We denote $\phi(G)$, or the **image** of ϕ to be the set of all $x \in H$ such that there's an $a \in G$ so that $\phi(a) = x$. Notice that $\ker \phi \trianglelefteq G$ and $\phi(G) \leq H$.

Definition 2.1.19 We call a chain of homomorphisms between groups an **exact sequence** if the image of one is the kernel of the next, and we call it a **short exact sequence** if it's of the form

$$0 \longrightarrow K \xrightarrow{i} G \xrightarrow{\pi} Q \longrightarrow 1$$

The existence of such a sequence (for K, Q, and G) is an alternative way of saying that G is an extension of K by Q.

Definition 2.1.20 We say that two extensions G and G' are **equivalent** if there is an isomorphism $\gamma : G \to G'$ such that the following diagram commutes:



γ is called an **isomorphism of extensions**, and it's not just an isomorphism between the groups themselves, it's also an isomorphism of "how" they extend K by Q.

We'll also need to talk a bit about coboundaries.

Theorem 2.1.21 For any two factor sets f and f' arising from transversals of the same group extension G realizing data (Q, K, θ), there's a function $h : Q \to K$ with $h(1) = 0$ such that

$$f'(x, y) - f(x, y) = xh(y) - h(xy) + h(x).$$

Proof. We know that $l'(q) - l(q) \in K$ since they're in the same coset of K, so denote $l'(q) - l(q) = h(q)$. This defines a function $h : Q \to K$, and it's not too hard to check that $h(1) = 0$. Next,

$$l'(x) + l'(y) = h(x) + l(x) + h(y) + l(y) = h(x) + xh(y) + l(x) + l(y) = h(x) + xh(y) + f(x, y) + l(xy)$$

$$= h(x) + xh(y) + f(x, y) - h(xy) + l'(xy).$$

Thus $f'(x, y) = h(x) + xh(y) + f(x, y) - h(xy)$, and since K is abelian, the result follows.□

Such an expression on the right is called a coboundary, and is a special type of factor set.

Definition 2.1.22 We call $g : Q \times Q \to K$ a **coboundary** if there's a function $h : Q \to K$ with $h(1) = 0$ such that

$$g(x, y) = xh(y) - h(xy) + h(x).$$

Coboundaries give us a new characterization of equivalent extensions.

Theorem 2.1.23 Let G and G' be extensions of K by Q. G and G' are equivalent iff they realize the same data (Q, K, θ) and there are factor sets f of G and f' of G' so that $f - f'$ is a coboundary.

Proof. First off, assume that G and G' are equivalent. Commutativity of the diagram gives $\gamma(a) = a$ for all $a \in K$. Moreover, if $x \in Q$, then for any transversal $l : Q \to G$,

$$x = \pi(l(x)) = \pi'\gamma(l(x)).$$

That is, $\gamma l : Q \to G'$ is another transversal. Applying γ to the equation $l(x) + l(y) = f(x, y) + l(xy)$ shows that γf is the factor set determined by the transversal γl. But since $f(x, y) \in K$ we know that $\gamma f = f$, meaning that f is also a factor set of G'. We can take $f' = f$ and $h(x) = 0$ for all x so that $h(1) = 0$ and

$$f'(x, y) - f(x, y) = xh(y) - h(xy) + h(x).$$

Conversely, suppose that there exist f, f' arising respectively from transversals l of G and l' of G' (with $l(1) = l'(1) = 0$), and a function $h : Q \to K$ with $h(1) = 0$ such that

$$f'(x, y) - f(x, y) = xh(y) - h(xy) + h(x).$$

Each element of G has a unique expression of the form $a + l(x)$, where $a \in K$ and $x \in Q$, and addition is given by

$$[a + l(x)] + [b + l(y)] = a + xb + f(x, y) + l(xy).$$

There's a similar description of addition in G'. Define $\gamma : G \to G'$ by

$$\gamma(a + l(x)) = a - h(x) + l'(x).$$

We know that $x = \pi(a + l(x))$, while

$$\pi'\gamma(a + l(x)) = \pi'(a - h(x) + l'(x)) = \pi'(l'(x)) = x.$$

Thus $\pi'\gamma = \pi$. Next, $i'(a) = i(a) = a$ for all $a \in K$; they're really embeddings and we just identify the three. Since $l(1) = 0$, we have $\gamma(a) = \gamma(a + l(1)) = a + h(1) + l'(1) = a$, for all $a \in K$. Thus all three functions act as the identity on K, so since i and i' have domain K, $i' = \gamma i$. The other composition cases can be computed based on this one, and you can see that the diagram commutes. Furthermore, it's not too hard to check that γ is a bijection, so what remains is to check that γ is a homomorphism. We see that

$$\gamma([a + l(x)] + [b + l(y)]) = \gamma(a + xb + f(x, y) + l(xy)) = a + xb + f(x, y) - h(xy) + l'(xy).$$

Next,

$$\gamma(a + l(x)) + \gamma(b + l(y)) = a - h(x) + l'(x) + b - h(y) + l'(y) = a - h(x) + xb - xh(y) + f'(x, y) + l'(xy)$$

$$= a + xb + f'(x, y) - xh(y) + h(xy) - h(x) - h(xy) + l'(xy) = a + xb + f'(x, y) - f'(x, y) + f(x, y) - h(xy) + l'(xy)$$

$$= a + xb + f(x, y) - h(xy) + l'(xy).$$

We got the same result so γ is a homomorphism, completing the proof.□

Definition 2.1.24 We denote $Z^2(Q, K, \theta)$ to be the set of all factor sets, and $B^2(Q, K, \theta)$ to be the set of all coboundaries.

It's not too hard to check that $Z^2(Q, K, \theta)$ forms an abelian group under $+$, where $(f+g)(x, y) = f(x, y)+g(x, y)$. $B^2(Q, K, \theta)$ forms a subgroup.

Definition 2.1.25 The **second cohomology group**, denoted $H^2(Q, K, \theta)$, is defined to be the quotient group $Z^2(Q, K, \theta)/B^2(Q, K, \theta)$. This is well-defined since all subgroups of abelian groups are normal.

Theorem 2.1.26 Let E be the set of equivalence classes of extensions G realizing data (Q, K, θ). If you define $\phi : H^2(Q, K, \theta) \to E$ so that $\phi(f + B^2) = G_f$, then ϕ is a bijection.

Proof. First of all, we need to check well-definedness since it could depend on the choice of representative f. We know that if $g \in f + B^2(Q, K, \theta)$ then f and g differ by a coboundary, so since f and g are factor sets of G_f and G_g respectively, we know that G_f and G_g are equivalent. Conversely, if G_f and G_g are equivalent, then there are factor sets f' of G_f and g' of G_g that are in the same coset. But by Theorem 2.1.21 we know that g' and g lie in the same coset, and so do f and f', so indeed $g \in f + B^2(Q, K, \theta)$. This shows that ϕ is well-defined and injective. Surjectivity is Theorem 2.1.15, thus ϕ is a bijection.□

So not only have we found out that G_f and G_g are equivalent when f and g differ by a coboundary, we can create a group structure on them where $G_f + G_g = G_{f+g}$, making ϕ an isomorphism!

3 Using the Method In Practice

So, to recap, we found a way to split extensions up via homomorphisms $\theta : Q \to \mathrm{Aut}(K)$, and we not only classified them, but we endowed them with a nice abelian group structure. Here's an example it to show how this works:

Let's compute all the extensions of C_3 by C_2. Call the elements of C_2 1 and a, and call the elements of C_3 $0, g$, and $2g$. For starters, what are the homomorphisms $\theta : C_2 \to \mathrm{Aut}(C_3)$? The automorphisms of C_3 are the ones that either preserve everything, which is the identity e, or invert everything, call that automorphism t. We know that $\theta(a)$ is either e or t, and both of these cases extend to homomorphisms (identity elements automatically map to identity elements under homomorphisms).

Next, all equivalence classes of factor sets $f : C_4 \times C_4 \to C_3$. We only need to determine $f(a, a)$ because we know the other values are 0. So set $f(a, a) = ng$ for some $n = 0, 1$, or 2. We can write $f(a^{m_1}, a^{m_2}) = nm_1m_2g$. In the case that $\theta(a) = e$, we know that θ is trivial, so the cocycle identity becomes

$$f(x, y) + f(xy, z) = f(y, z) + f(x, yz).$$

For what n is this true? Well, letting $x = a^{m_1}$, $y = a^{m_2}$, and $z = a^{m_3}$, we get

$$nm_1m_2g + n(m_1 + m_2)m_3g = nm_2m_3g + nm_1(m_2 + m_3)g.$$

Distributing and commuting the terms, we see that this is true no matter what n is. How about the coboundaries? We'll denote them F instead of g since we already have a g. Again, we only need to look at $F(a, a)$ since the other values are 0. We compute that:

$$F(a, a) = ah(a) - h(a^2) + h(a) = h(a) - 0 + h(a) = 2h(a).$$

Of course, $h(a)$ could be anything, which means $2h(a)$ could be anything since $h(a)$ has order dividing 3 thus $2 \cdot 2h(a) = 4h(a) = h(a)$. But the same was true for $f(a, a)$, so actually the coboundaries are all the factor sets! Thus $H^2(C_2, C_3, \theta)$ is trivial and the operation on the only extension is

$$(k_1, q_1) + (k_2, q_2) = (k_1 + q_1k_2 + f(q_1, q_2), q_1q_2) = (k_1 + k_2, q_1q_2).$$

This is the direct product $C_2 \times C_3 \cong C_6$.

If $\theta(a) = t$, then again we let $f(a, a) = ng$, we note that $f(a^{m_1}, a^{m_2}) = nm_1m_2g$, and we figure out for which n the following equation holds:

$$nm_1m_2g + n(m_1 + m_2)m_3g = (-1)^{m_1}nm_2m_3g + nm_1(m_2 + m_3)g.$$

Plugging in $m_1, m_2, m_3 = 1$, we get that

$$ng + 2ng = -ng + 2ng,$$

or

$$0 = ng.$$

This means that $n = 0$, so $Z^2(Q, K, \theta)$ is trivial and automatically $H^2(Q, K, \theta)$ is trivial. As before, the unique extension is the semidirect product with action θ, which is denoted D_3.

Now, one minor problem is that, although we classified equivalent extensions nicely, it turns out that isomorphic extensions are not necessarily equivalent. That is, a group G can be an extension of K by Q in multiple ways. Another problem, this time major, is of course that we've only done this in the case that K is abelian. What if K isn't abelian?

4 Computing a Case Where K is Nonabelian

There's no general method for any K and Q including nonabelian K, which is why the Group Extension Problem is unsolved. Although, it's not like you can't do any nonabelian cases. For one thing, if Q is trivial then K is the only extension of K by Q. Also, if K and Q are small, like say $K = D_3$ and $Q = C_2$ (smallest nonabelian nontrivial case), then the extensions are not too hard to compute through brute force (once you know the groups of order 12). In fact, let's do that!

To start, the five different groups of order 12 are: C_{12}, $C_6 \times C_2$, D_6, A_4, and Q_{12}.

Definition 4.1 The **dyciclic group** Q_{12} has elements $\{e, a, \cdots, a^5, x, xa, \cdots, xa^5\}$ where $a^n \cdot a^m = a^{n+m \pmod 6}$, $xa^n \cdot a^m = xa^{n+m \pmod 6}$, $a^n x a^m = x a^{m-n \pmod 6}$, and lastly $xa^n xa^m = a^{m-n+3 \pmod 6}$.

Definition 4.2 The **diahedral group** D_6 is the semidirect product $C_6 \times_\theta C_2$ where $\theta(1) = 0$ and $\theta(a)$ is the inversion automorphism, similarly to D_3.

Now, C_{12} and $C_6 \times C_2$ can be immediately discarded because abelian groups cannot have nonabelian subgroups. If A_4 was an extension of D_3 by C_2, then R would have to be a 3-cycle and T would have to be a double transposition. But those together actually generate all of A_4, so we may discard A_4.

Now, what about D_6? Well, letting $D_3 = \langle R^2, T\rangle$ and $\langle R^3\rangle$, we see that D_6 is actually the direct product of D_3 and C_2. But also, if we choose $C_2 = \langle RT\rangle$, then it turns out conjugacy by RT switches R and R^2, switches T and R^2T, but preserves e and R^4T, so just a semidirect product. This is an example of how isomorphic extensions are not necessarily equivalent, though in it K is nonabelian.

As for Q_{12}, we know that

$$xa^n xa^n = a^{n-n+3} = a^3$$

for all n. So since a^3 has order 2, we know that xa^n has order 4. Thus, since R has order 3 and T has order 2, T has to be a^3 and R has to be a^2 or a^4. But that means they generate C_6, a contradiction. So D_6 is the only extension of D_3 by C_2.

5 Ways to attack this problem when K is nonabelian

The method we have is only useful when K is abelian- abelian groups are only a small section of all the groups. And it's not practical to attack everything through brute force. So let's explore some theorems that help in certain cases when K is nonabelian.

First, we'll need some definitions (and a theorem):

Definition 5.1 We say that K is a **Hall** subgroup of G, named after P. Hall, if $\gcd(|K|, |G|/|K|) = 1$. That is, if $|K| = n$ and $|G| = mn$ then $\gcd(n, m) = 1$.

Definition 5.2 Let G be a group and let K and Q be subgroups. If $K \cap Q = \{e\}$ and $KQ = G$, then we say that K and Q are **complements** of each other. Note that if $K \trianglelefteq G$ then G is an inner semidirect product of K and Q.

Definition 5.3 Let $K_1, K_2 \leq G$. We say that K_1 and K_2 are **conjugate** if there's a $g \in G$ such that if $k \in K_1$ then $gkg^{-1} \in K_2$ and $a : K_1 \to K_2$ defined by $a(k) = gkg^{-1}$ is a bijection. Compare this to conjugation by g: it's the same except with elements instead of subgroups.

Definition 5.4 A p-**group** G is a group such that every element of G has order a power of p. A **Sylow** p-**subgroup** of a group G is a p-subgroup P such that there's no p-subgroup $P' > P$. That is, P is maximal.

Definition 5.5 Let G be a group, X a set, and $\star : G \times X \to X$ an operation. That is, $\star$ takes in a thing from G and a thing from X and outputs a thing in X. We call $\star$ a **group action** that G has on X if $e \star x = x$ and $(g \cdot h) \star x = g \star (h \star x)$.

Definition 5.6 Let $\star$ be a group action of a group G on a set X, and let $x \in X$. The **orbit** of x, denoted $\text{orb}(x)$ is the set of all elements in X of the form $g \star x$ for some $g \in G$.

Definition 5.7 Let $g \in G$, $x \in X$, and $\star$ be a group action. We say g **fixes** x, or x is **fixed** by g if $g \star x = x$. We denote $\text{fix}(g)$ to be the set of all x that are fixed by g, and $\text{stab}(x)$, called the **stabilizer** of x to be the set of all g that fix x. Notice that $\text{fix}(g) \subseteq X$ and $\text{stab}(x) \leq G$ (not necessarily normal).

Theorem 5.8 Let $\star$ be an action of G on X and let $x \in X$. Then $|\text{orb}(x)||\text{stab}(x)| = |G|$. This is called the **orbit-stabilizer theorem**.

Here's a result:

Theorem 5.9 Let K be an abelian normal Hall subgroup of a group G. Then K has a complement in G.

Remark. I know we said that K wouldn't have to be abelian, and K doesn't for this theorem to be true, but we need to prove this first before we can get to that.

Proof. Let $|K| = m$, let $Q = G/K$, and let $|Q| = n$, so that $\gcd(m, n) = 1$. It suffices to prove that every factor set $f : Q \times Q \to K$ is a coboundary. Define $\sigma : Q \to K$ by

$$\sigma(x) = \sum_{y \in Q} f(x, y).$$

This is well-defined since Q is finite and K is abelian. Sum the cocycle identity

$$xf(y, z) - f(xy, z) + f(x, yz) = f(x, y)$$

over all z to obtain

$$x\sigma(y) - \sigma(xy) + \sigma(x) = nf(x, y)$$

(as z ranges over all of Q, so does yz). Since $\gcd(m, n) = 1$, there are integers s and t with $sm + tn = 1$. Define $h : Q \to K$ by $h(x) = t\sigma(x)$. Then $h(1) = 0$ and

$$xh(y) - h(xy) + h(x) = f(x, y) - msf(x, y).$$

But since $sf(x, y) \in K$ we know that $msf(x, y) = 0$, thus f is a coboundary.□

Example 5.10 Let's prove that C_{15} is the only group of order 15. There's a theorem we're going to use called **Cauchy's Theorem**, which is sort of like a converse to Lagrange's Theorem:

Theorem 5.11 Let G be a group and let $p \big| |G|$. Then G has an element of order p.

Corollary 5.12 A finite group is a p-group iff its order is a power of p.

Now, take any group G of order 15. Using this theorem, we know that G has an element a of order 5 and an element b of order 3. Since every power of a has order 5 except e and any power of b has order 3 except e, we know that $\langle a \rangle \cap \langle b \rangle = \{e\}$ (recall that $\langle g \rangle$ denotes the subgroup of powers of g). Now, let's show that if $a^{x_1} b^{y_1} = a^{x_2} b^{y_2}$ then $x_1 \equiv x_2 \pmod 5$ and $y_1 \equiv y_2 \pmod 3$, that is $a^{x_1} = a^{x_2}$ and $b^{y_1} = b^{y_2}$. Multiplying on the left by a^{-x_2} and on the right by b^{-y_1} gives

$$a^{x_1 - x_2} = b^{y_2 - y_1}.$$

But since $\langle a \rangle \cap \langle b \rangle = \{e\}$, we know that $a^{x_1 - x_2} = b^{y_2 - y_1} = e$, so $a^{x_1} = a^{x_2}$ and $b^{y_1} = b^{y_2}$. Thus $\langle a \rangle \langle b \rangle$ has 15 elements which means that it must be the whole group G. Thus $\langle a \rangle$ and $\langle b \rangle$ are complements. But suppose $\langle a \rangle$ is not normal. That means that $\langle bab^{-1} \rangle \cap \langle a \rangle = \{e\}$. Why? Well, otherwise, they intersect somewhere other than e, so $ba^n b^{-1} = (bab^{-1})^n = a^m$ for some m, n not congruent to 0 mod 5. But we could then raise to the power of n's multiplicative inverse mod 5 (since $n \not\equiv 0$ and 5 is prime), so $bab^{-1} = a^m$. Since conjugation by b^2 is just conjugation by b compose conjugation by b and since conjugation by e does nothing, we know that their intersection is $\{e\}$ after all. But then by the same logic as earlier, $\langle a \rangle \langle bab^{-1} \rangle$ has 25 elements, a contradiction since G only has 15.

Thus $\langle a \rangle$ is normal and $G = \langle a \rangle \rtimes \langle b \rangle$. However, it turns out that $\text{Aut}(C_5) = C_4$, and the only homomorphism $\theta : C_3 \to C_4$ is the one that sends everything to e, also called the trivial homomorphism. Why is that

the only homomorphism? Well, because e is the only element x of C_4 such that $x^3 = e$, which holds true for the elements of C_3, and homomorphisms need to preserve that.

Indeed, C_5 is a normal Hall subgroup of C_{15} and C_3 is a complement.

Before we can remove the abelianess condition, we have some stuff to mention.

Definition 5.13 Let G be a group. We denote $Z(G)$, called the **center** of G to be the subset of all elements $z \in G$ that **commute** with everything, that is for all $x \in G$, $zx = xz$.

Definition 5.14 Let $Q \leq G$. The **normalizer** of Q in G, denoted $N_G(Q)$ is the set of all $g \in G$ such that $gQg^{-1} = Q$. Note that $N_G(Q) \leq G$ and $Q \trianglelefteq N_G(Q)$. We also define $C_G(Q)$, called the **centralizer** of Q in G to be the set of all $g \in G$ such that for any $q \in Q$, $gq = qg$, or $gqg^{-1} = q$. Note that $C_G(Q) \leq N_G(Q)$ and that $C_G(Q) \cap Q = Z(Q)$.

Theorem 5.15 Let K be a normal subgroup of a finite group G. If P is a Sylow p-subgroup of K for some prime p, then

$$G = KN_G(P).$$

This is called the **Frattini Argument**.

Theorem 5.16 Let $\phi : G \to H$ be a homomorphism. Then

$$G/\ker(\phi) \cong \phi(G).$$

Theorem 5.17 Let $N \trianglelefteq G$ and $K \leq G$. Then $N \trianglelefteq NK \leq G$, $N \cap K \trianglelefteq K$, and

$$NK/N \cong K/N \cap K.$$

Theorem 5.18 Let $H \trianglelefteq G$ and let $T \leq K$ such that $T \trianglelefteq G$. Then $T \trianglelefteq K$ and

$$(G/T)/(K/T) \cong G/K.$$

Theorem 5.19 Let $N \trianglelefteq G$. There is a bijection from the set of subgroups of G containing N to the set of subgroups of G/N sending K to K/N. Furthermore, $K \trianglelefteq G$ is normal iff $K/N \trianglelefteq G/N$.

These are called the **four isomorphism theorems**, stated in order from first to fourth.

Lemma 5.20 Let P be a p-group. Then the center $Z(P) \neq 1$.

Now we remove the condition that K is abelian.

Theorem 5.21 Let K be a normal Hall subgroup of a group G. Then K has a complement in G.

Proof. Let $|K| = m$ and let $|G| = mn$ so that $\gcd(m, n) = 1$. We prove, by induction on $m \geq 1$, that G contains a subgroup of order n. The base step is trivially true (take $\{e\}$). If K contains a nontrivial subgroup T which is normal in G, then $K/T \trianglelefteq G/T$ and

$$|(G/T)/(K/T)| = (|G|/|T|)/(|K|/|T|) = |G|/|K| = n,$$

so that K/T is a normal Hall subgroup of G/T (because $|K/T||K| = m$). If $|K/T| = m'$, then $m' < m$ and $[G/T : K/T] = n$. The inductive hypotheses gives a subgroup $N/T \leq G/T$ of order n. So then $|N| = n|T|$ and

$\gcd(n, |T|) = 1$ (since $|T|$ divides m), so that T is a normal Hall subgroup of N (with $|T| < m$ and with index $[N : T] = n$). By induction, N and hence G contains a subgroup of order n.

We can now assume that K is a minimal normal subgroup of G. If p is a prime dividing m and if P is a Sylow p-subgroup of K, then the Frattini argument gives $G = KN_G(P)$. By the second isomorphism theorem,

$$G/K = KN_G(P)/K \cong N_G(P)/(K \cap N_G(P)) = N_G(P)/N_K(P)$$

so that $|N_K(P)|n = |N_K(P)||G/K| = |N_G(P)|$. If $N_G(P)$ is a proper subgroup of G then $|N_K(P)| < m$, and induction shows that $N_G(P)$ contains a subgroup of order n. Thus we can assume that $N_G(P) = G$, that is, $P \trianglelefteq G$.

Since $K \geq P$ and K is a minimal normal subgroup of G, we have that $K = P$ ($P \neq \{e\}$ since $p|m$.) By what we'll see later, $Z(P) \trianglelefteq G$ as well. Minimality applies again, and $Z(P) = P$ (we know $Z(P) \neq 1$ because P is a finite p-group). But that means $P = K$ is abelian, and the proof follows from Theorem 5.9 (since a complement must have order n).

So we have $Q \leq G$ has order n. The only order of any possible element in $K \cap Q$ is 1 since $\gcd(m, n) = 1$. But e is the only element of order 1 of any group, so $K \cap Q = \{e\}$. Then, using similar logic to Example 5.10, we have that KQ generates mn distinct elements thus all of G. This means that Q is a normal complement of K.□

Note: We said, "by what we'll see later, $Z(P) \trianglelefteq G$ as well." This is why it's true:

Definition 5.22 Let $H \leq G$. We say that H is **characteristic**, denoted H char G, if every automorphism ϕ of G **preserves** H, that is $\phi(H) = H$ ($\phi(H)$ is the image of ϕ restricted to H). It's checkable that conjugation is an automorphism, so all characteristic subgroups are normal (preserved under conjugation).

Since automorphisms preserve commutativity, we know that $Z(G)$ is characteristic.

Lemma 5.23 If H char G and K char H then K char G. If $H \trianglelefteq G$ and K char H then $K \trianglelefteq G$ (note that if $H \trianglelefteq G$ and $K \trianglelefteq H$ this doesn't necessarily mean $K \trianglelefteq G$).

Proof. As for the first case, take any automorphism ϕ of G. We know that $\phi(H) = H$ since H char G, so $\phi|_H$ (denoting ϕ restricted to H) is an automorphism of H. Thus $\phi(K) = \phi_H(K) = K$ and K char G.

As for the other part, take any $g \in G$. Since $H \trianglelefteq G$ we know $gHg^{-1} = H$ so ϕ, denoting conjugation by g restricted to H, is an automorphism of H. Thus $gKg^{-1} = \phi(K) = K$ and $K \trianglelefteq G$.□

Thus since $P \trianglelefteq G$ and $Z(P)$ char P, we know $Z(P) \trianglelefteq G$.

Here's a further theorem about normal Hall subgroups.

Theorem 5.24 Let K be an abelian normal Hall subgroup of a group G. Then all complements of K are conjugate.

Proof. Again we denote $|K|$ by m and $|G/K|$ by n, and $\gcd(m, n) = 1$. Let Q_1 and Q_2 be complements of K. It's not too hard to check that there are transversals $l_i : G/K \to G$, for $i = 1, 2$, with $l_i(G/K) = Q_i$ and with each l_i a homomorphism. It follows that the factor sets f_i arising from l_i (respectively) are identically zero. If we define $h(x) = l_1(x) - l_2(x)$, then

$$0 = f_1(x, y) - f_2(x, y) = xh(y) - h(xy) + h(x).$$

Summing over all $y \in G/K$ gives the following equation in K:

$$0 = xa_0 - a_0 + nh(x),$$

where $a_0 = \sum_{y \in G/K} h(y)$. Let $sm + tn = 1$ and define $b_0 = ta_0$. Since K has order m,

$$-h(x) = smh(x) - h(x) = -tnh(x) = xta_0 - ta_0 = xb_0 - b_0$$

for all $x \in G/K$. We claim that $-b_0 + Q_1 + b_0 = Q_2$. If $l_1(x) \in Q_1$, then

$$-b_1 + l_1(x) + b_0 = -b_0 + xb_0 + l_1(x) = -h(x) + l_1(x) = l_2(x) - l_1(x) + l_1(x) = l_2(x).\square$$

Again, we'll need a bit of background before we can remove the abelianess condition.

Definition 5.25 An **elementary p-group** is a group G with all elements having order 1 or p. An **elementary abelian p-group** is an elementary p-group that is abelian.

Definition 5.26 A **minimal normal subgroup** of a group G is a normal subgroup $N \neq \{e\}$ such that there's no normal subgroup $K \trianglelefteq G$ with $\{e\} < K < N$.

Theorem 5.27 If G is a finite solvable group, then every minimal normal subgroup of G is an elementary abelian p-group for some prime p.

Definition 5.28 Let G be a group. The **commutator subgroup** of a group G, denoted G', is the generating group of the set of **commutators**, that is the elements of the form $aba^{-1}b^{-1}$.

This next lemma is called the **Dedikind Law**:

Lemma 5.29 Let H, K, and L be subgroups of G with $H \leq L$. Then $HK \cap L = H(K \cap L)$ (we don't assume either HK or $H(K \cap L)$ is a subgroup).

Theorem 5.30 Let P be a Sylow p-subgroup of a finite group G.

(i) If there are r Sylow p-subgroups in the conjugacy class of P, then r is a divisor of $|G|$ and $r \equiv 1 \pmod{p}$.
(ii) All Sylow p-subgroups are conjugate to P.
(iii) The amount of Sylow p-subgroups of G is a divisor of $|G|$ conjugate to 1 mod p.

That's called the **Sylow Theorem**.

Now we can reduce the conditions, but a bit less this time.

Theorem 5.31 Let K be a normal Hall subgroup of a group G. If at least one of K or G/K is solvable, then all complements of K are conjugate.

Proof. Let $|K| = m$, let $|G/K| = n$, and let Q_1 and Q_2 be complements of K in G. Using induction on $|G|$, the base case is trivial.

As for induction, first off, assume that K is solvable. Since K' char K and $K \trianglelefteq G$, again by Lemma 5.23 $K' \trianglelefteq G$. Furthermore, $Q_1K'/K' \cong Q_1/(Q_1 \cap K') \cong Q_1$ (because $Q_1 \cap K' \leq Q_1 \cap K = \{e\}$), so that $|Q_1K'/K'| = n$. We know that $K' < K$ since K is solvable. If $K' = 1$, then K is abelian and again the result is Theorem 5.24. Otherwise, $|G/K'| < |G|$, and the inductive hypotheses shows that the subgroups Q_1K'/K' and Q_2K'/K' are conjugate in G/K'. Thus there's a $\overline{g} \in G/K'$ with $\overline{g}(Q_1K'/K')\overline{g}^{-1} = Q_2K'/K'$, so then $gQ_1g^{-1} \leq Q_2K'$ (where $gK' = \overline{g}$). But $K' < K$ gives $|Q_1K'| < |G|$, so the subgroups gQ_1g^{-1} and Q_2 of order n are conjugate in Q_2K', thus are conjugate in G (showing Q_1 and Q_2 are conjugate as well).

Now assume that G/K is solvable. Let M/K be a minimal normal subgroup of G/K. Since $K \leq M$, the Dedekind law gives

$$M = M \cap G = M \cap Q_iK = (M \cap Q_i)K$$

for $i = 1, 2$. Note also that $M \cap Q_i \trianglelefteq Q_i$. Then, solvability of G/K gives that M/K is an elementary abelian p-group for some prime p by Theorem 5.27. If $M = G$, then G/K is an elementary abelian p-group, and since M/K is a minimal normal subgroup it's not too hard to see that $|M/K| = p$ (therefore $|G/K| = p$). Thus Q_1

and Q_2 ($\cong G/K$) have to be Sylow p-subgroups of G since they're Hall subgroups, and hence they're conjugate by the Sylow theorem.

Thus we can assume that $M < G$. We know $M \cap Q_i$ is a complement of K in M since $M = (M \cap Q_i)K$ and $(M \cap Q_i) \cap K \leq Q_i \cap K = 1$. By the inductive hypotheses there is $x \in M \leq G$ with $M \cap Q_1 = x(M \cap Q_2)x^{-1} = M \cap xQ_2x^{-1}$. If we denote $J = M \cap Q_1$, then $J \trianglelefteq Q_1$, and so

$$Q_1 \leq N_G(J).$$

Two applications of the Dedikind Law give

$$N_G(J) = N_G(J) \cap KQ_1 = (N_G(J) \cap K)Q_1$$

and

$$J[N_G(J) \cap K] \cap Q_1 = J([N_G \cap K] \cap Q_1) = J$$

(because $(N_G(J) \cap K) \cap Q_1 \leq K \cap Q_1 = 1$). Thus Q_1/J is a complement of $J(N_G(J) \cap K)/J$ in $N_G(J)/J$. By similar logic and the fact that $M \cap xQ_2x^{-1} = M \cap Q_1$, we know that xQ_2x^{-1}/J is a complement of $J(N_G(J) \cap K)/J$ in $N_G(J)/J$ as well. By the inductive hypotheses, there is $\overline{y} \in N_G(J)/J$ with $Q_1/J = \overline{y}(xQ_2x^{-1}/J)\overline{y}^{-1}$. It follows that $Q_1 = yxQ_2x^{-1}y^{-1}$, where $yJ = \overline{y}$, as desired.□

It turns out that a theorem called the **Feit-Thompson theorem** removes the solvability part entirely:

Theorem 5.32 All groups of odd order are solvable (!)

Since $|K|$ and $|G/K| = |G|/|K|$ are relatively prime, by this theorem at least one of them must be odd so either K or G/K is solvable. Thus we may remove that condition, giving us a unified theorem:

Theorem 5.33 Let K be a normal Hall subgroup of a group G. Then K has a complement in G and all complements are conjugate.

We mentioned a theorem called the Sylow Theorem, and it is very useful. Its proof is quite nice, so let's prove it. We'll first need a lemma.

Lemma 5.34 Let P be a Sylow-p subgroup of a finite group G.

(i) $|N_G(P)/P|$ is coprine to p, that is their gcd is 1.
(ii) If $a \in G$ has order some power of P and $aPa^{-1} = P$, then $a \in P$.

Proof. (i) If they're not coprime, the only possibility is that $p \big| |N_G(P)/P|$. Then Cauchy's theorem shows that $N_G(P)/P$ contains some element aP of order P. Thus $S^\star = \langle aP \rangle$ has order p. If you take the union over $S^\star$ and call it S, it's not too hard to check that this is a subgroup (of $N_G(P)$) since it's just all the elements from some coset of $\langle aP \rangle$. Since $|S| = |S^\star||P| = p|P|$, we know that S is a p-group. But $S > P$, so this contradicts the fact that P is Sylow.

(ii) To start, we know that $a \in N_G(P)$ since $aPa^{-1} = P$. So suppose $a \notin P$. Then $aP \neq P$. Since $|aP| \big| |a|$ (which you can check), we know that $|aP|$ is a power of p, so since $|aP| \neq 1$ we know $|aP|$ is a multiple of P. This contradicts (i) by Lagrange's theorem.□

Proof of Sylow Theorem. (i) Let $X = \{P_1 \cdots P_r\}$ be the set of all conjugates of P, where P is denoted by P_1 here. If we take $g \star P_i = gP_ig^{-1}$, this is a group action of G on X (and X is an orbit). If you take any Sylow p-subgroup Q of G, you can restrict $\star$ to Q and that would still be a group action. By the orbit-stabilizer theorem all of the orbits under this action have to have order dividing $|Q|$, thus a power of p. What would it mean to say that one of these orbits has size 1? If we call it $\{P_i\}$, then any element $q \in Q$ would be such that $qP_iq^{-1} = P_i$. But then by our lemma, $q \in P_i$ and $Q \leq P_i$. But since Q is Sylow we know $Q = P_i$. Taking Q to be $P_1 = P$ we have that $\{P_i\}$ can't be an orbit unless $i = 1$ (in which case it is), so that's the only orbit of size

1. But then since the other orbit sizes are powers of p we know they must be multiples of p, so if you union the orbits you get that

$$r = |X| = 1 + kp$$

for some k (since everything must be in some orbit). That is,

$$r \equiv 1 \pmod{p}.$$

We know that the action of G on X has only one orbit by definition of X, so again the orbit-stabilizer theorem gives $r = |X||G|$.

(ii) Suppose there were a Sylow p-subgroup Q not conjugate to P, that is $Q \notin X$. Then, by what we've seen any orbit size is a power of p not equal to 1, meaning all orbits have size a multiple of p. But that means $r \equiv 0 \pmod{p}$, contradicting the previous congruence.

(iii) By (ii), we know X contains all Sylow p-subgroups of G, so r is the amount of them. The result follows from (i).□

It's not too hard to check that conjugates of Sylow p-subgroups are Sylow p-subgroups themselves (Hint: Conjugation is an automorphism), so the Sylow p-subgroups are a conjugacy class.

We'll also talk a bit about wreath products.

Let's say you have a chandelier with m arms and n lights arranged on each arm. What is the group of ways in which you can twist the chandelier around, where you can rotate the arms on it and separately rotate the lights on each arm (operation is composition)? Well, this is an example of a Wreath Product.

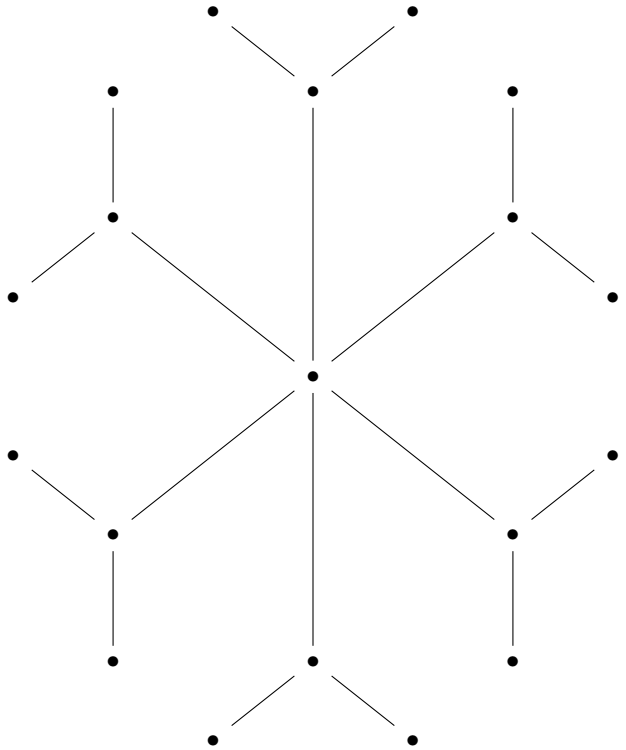
Definition 5.35 Take two groups D and Q, a set $\{D_\omega\}$ of isomorphic copies of D indexed by a set Ω, and take a group action $\star$ that Q has on Ω. You define the wreath product of D and Q, denoted $D \wr Q$, to be the semidirect product of $\Pi_{\omega\in\Omega} D_\omega$ (this is the direct product) and Q, with an action $\cdot$ defined by $q \cdot (d_\omega) = (d^q_\omega)$, where d^q_ω is the element in $D_{q^{-1}\star\omega}$ corresponding to d_ω (since the groups are isomorphic).

What's basically happening is that Q represents the rotations of the arms, Ω represents the arms, $\star$ represents the action Q has on the arms, and D_ω represents the rotations of the lights on the arm represented by ω. These rotation groups should all be isomorphic, and our action of Q on K is basically just moving the rotations on the clusters of lights so they rotate another cluster of lights instead (depending on the permutation q imposes).

Here's another example where the wreath product comes up as a symmetry group.

Definition 5.36 A **graph** is a set V, called **vertices**, combined with an **adjacency** relation on V denoted $v \sim u$, a relation that is symmetric ($v \sim u$ implies $u \sim v$) and irreflexive ($v \not\sim v$).

Example 5.37 Consider the diagram below.



The symmetry group of this graph would be all permutations of the vertices that preserve the connections. The center vertex is the only vertex with six connections, the others have 1 or 3, so it stays where it is. The slightly outer vertices with 3 connections permute, and each vertex branching out of one of those goes to a vertex branching out of its image under the permutation. As before, this is a wreath product $S_2 \wr S_6$.

The following theorem (and definition) show how it's relevant to the Group Extension Problem.

Definition 5.38 The regular wreath product $D \wr_r Q$ is the wreath product with $\Omega = Q$ and $\star$ defined such that $g \star h = g \cdot h$.

Here's a neat theorem about regular wreath products.

Theorem 5.39 If D and Q are groups (with D not necessarily abelian) then the regular wreath product contains an isomorphic copy of every extension of D by Q. In other words, there's an injective homomorphism from every extension of K by Q to $D \wr_r Q$.

Proof. If G is an extension of D by Q, then there is a surjective homomorphism $G \to Q$ with kernel D, which we denote by a mapping to $\overline{a}$. Choose a transversal $l : Q \to G$.

For $a \in G$, define $\sigma_a : Q \to D$ by $\sigma_a(x) = l(x)^{-1} a l(\overline{a^{-1}x})$. (We treat this as an element of K: Basically, you choose $\sigma_a(q)$ for the coordinate in D_q.) To see that this actually maps into D,

$$l(x)^{-1} a l(\overline{a^{-1}x}) D = l(x)^{-1} a l(\overline{a^{-1}}) l(x) D = l(x)^{-1} a l(\overline{a^{-1}}) D l(x) = l(x)^{-1} a a^{-1} D l(x) = l(x)^{-1} D l(x) = D.$$

Thus $\sigma_a(x) \in D$. If $q \in Q$, denote σ_a^q to be q acting on $\sigma_a \in K$. Then, if $a, b \in G$ we have

$$\sigma_a(x) \sigma_b^{\overline{a}}(x) = \sigma_a(x) \sigma_b(\overline{a^{-1}}x) = l(x)^{-1} a l(\overline{a^{-1}}x) l(\overline{a^{-1}}x)^{-1} b l(\overline{b^{-1}a^{-1}}x) = l(x)^{-1} ab l((\overline{a}\overline{b})^{-1}x) = \sigma_{ab}(x).$$

This leads us to define $\phi : G \to D \wr_r Q$ by

$$\theta(a) = (\sigma_a, \overline{a}).$$

Our equation above shows that ϕ is a homomorphism:

$$\phi(a)\phi(b) = (\sigma_a, \overline{a})(\sigma_b, \overline{b}) = (\sigma_a \sigma_b^{\overline{a}}, \overline{a}\overline{b}) = (\sigma_{ab}, \overline{ab}) = \phi(ab).$$

Finally, we show ϕ is injective. If $a \in \ker \phi$, then $\overline{a} = 1$ and $\sigma_a(x) = 1$ for all $x \in Q$. The second equation gives $\sigma_a(x) = l(x)^{-1} a l(\overline{a^{-1}} x) = 1$. Since $\overline{a} = 1$, we know that $\overline{a^{-1}} = 1$, so the equation says that $l(x)^{-1} a l(x) = 1$. Thus $a = 1$.□

Corollary 5.40 If S is a class of finite groups closed under subgroups and semidirect products (i.e. if $A \in S$ and $C \leq A$ then $C \in S$ and if $A, B \in S$ then $A \rtimes_\theta B \in S$ for all θ), then S is closed under group extensions.

Proof. Suppose G is an extension of K by Q, where both $D, Q \in S$. Since S is closed under semidirect products, it is closed under finite direct products. Hence, $K = \Pi_{q \in Q} D_q \in S$. Again since S is closed under semidirect products, the wreath product $D \wr_r Q = K \rtimes Q \in S$. Lastly, since S is closed under subgroups, the theorem gives $G \in S$.□

For more details about this topic and more different approaches, you could look at [4]. To see a more module-theoretic approach, read [3]. You can also find more details in [1].

Acknowledgments. I would like to thank my teacher Simon Rubinstein-Salzedo for making the writing of this paper possible, and my T.A. Kishan Jani for his help along the way.

References

[1] Zachary W Adams. *The Group Extensions Problem and Its Resolution in Cohomology for the Case of an Elementary Abelian Normal Sub-group*. PhD thesis, Colorado State University, 2018.

[2] Timothy Gowers, June Barrow-Green, and Imre Leader. *The Princeton companion to mathematics*. Princeton University Press, 2010.

[3] RAPHAEL HO. Classification of group extensions and h2.

[4] Joseph J Rotman. *An introduction to the theory of groups*, volume 148. Springer Science & Business Media, 2012.