Semidirect Products, Group Extensions, Split Exact Sequences, and all that

Contents

1 Some points of terminology

- The identity element generally is denoted 0 for an abelian group, 1 for a nonabelian group, and e for a general group. Similarly, we typically employ additive notation for abelian groups and multiplicative notation for nonabelian (or general) groups.
- The trivial group usually is denoted by the same symbol as identity, which is the only element it contains. It should *not* be confused with the empty set. So, if we write $G = 0$ we mean the trivial group, and if we write $g = 0$ we mean the identity element of an abelian group.
- On a similar note, when we speak of "disjoint" subgroups H and K we mean that $H \cap K$ is the trivial group, not the null set (otherwise, their intersection would not be a group).
- There only is one homomorphism from a trivial group to any other group, and it is injective: $f(e) = e'$. There only is one homomorphism from any group to a trivial group, and it is surjective: $f(g) = e'$. Put another way, the trivial group is both the initial and terminal object in the category GRP.

  Although here we distinguish the identities of the groups, usually we'll just say e for all groups involved and it will be clear from the context which it belongs to.
- Unless otherwise specified, when we write $H \subset G$ for group G, H will be a subgroup, not just a subset.

- The notation HG commonly is used in two ways.
  - When H and G are subgroups of the same group (or $H \subset G$), HG is the set of all products of elements from H and G (i.e. $\{(h \cdot g); h \in H, g \in G\}$). Likewise, gH is the set $\{(g \cdot h); h \in H\}$ for the given g (and similarly for Hg).
  - When H and G are unrelated groups, HG will denote the *set* of all pairs $\{(h, g); h \in H, g \in G\}$ without any implied group structure. I.e. the forgetful functor applied to $H \times G$.
- Recall that $Aut(G)$ is the group of isomorphisms $G \to G$.

  Automorphisms should not be confused with endomorphisms. Endomorphisms are homomorphisms $G \to G$, whereas automorphisms are isomorphisms $G \to G$. Every automorphism is an endomorphism, but not every endomorphism is an automorphism (it would have to be bijective as well).
- The term "direct product" and "direct sum" tend to be used interchangeably (along with the notation $\oplus$ and $\times$ sometimes). We'll reserve $\times$ for the setwise direct-product and use $\oplus$ for the group direct sum. Direct products and direct sums of groups are the same for finite index-sets. I.e. unless we are taking a direct sum over an infinite number of groups, it is the same as the direct product.

  What about the case of an infinite number of groups? Let J be the relevant index set and let's denote the groups G_j (for $j \in J$). An element of the direct product $\times_{j \in J} G_j$ consists of a choice of element g_j from each of the G_j's. An element of the direct sum $\oplus_{j \in J} G_j$ consists of the same but with the constraint that all but a finite number of those g_j's are the identity elements of their respective G_j's. I.e., only a finite number of the entries are non-trivial.
- Group isomorphism is denoted $\approx$.
- For convenience, we'll use the notation $Iso(G, H)$ to denote the set of isomorphisms $G \to H$. This obviously is not a group unless $G = H$, in which case it is just $Aut(G)$.

2 A Review of Some Group Theory

For our discussion we'll need a clear understanding of normal subgroups and quotient groups as well as a few other concepts from group theory, so let's review these.

2.1 Basic Definitions

First, a brief refresher on Normal subgroups and Quotient groups. Suppose we are given group G and subgroup $H \subseteq G$.

- **Left cosets** are written gH and **right cosets** are written Hg. Each is a set of elements in G.

  Not all left cosets are distinct, but any two are either equal or disjoint. Ditto for right cosets.
- The left (right) cosets form a partition of G, but they do not in general form a group.

  We can try to imbue them with a suitable product, but there are obstructions to the group axioms. For example $g^{-1}H$ is not a useful inverse since $(gh)^{-1} = h^{-1}g^{-1}$, so neither left cosets nor right cosets multiply as desired. More generally $(gg')H$ does not consist of a product of an element of gH and an element of $g'H$.
- In general, the partitions formed from the left and right cosets are different. I.e., the set of left cosets need not equal the set of right cosets.

  This is not a vacuous statement. Even if $gH \neq Hg$ for individual g's, it is conceivable that $gH = Hg'$ for some g' associated with each g. However, this is not the case in general.
- The **Quotient Set** G/H is the set of left cosets. As mentioned, it is not a group in general.

  There is an equivalent definition for right cosets, written $H \setminus G$, but it doesn't appear often. Every result involving one has an analogue involving the other, so the preference is a matter of convention. In most cases that we care about the two will be the same, so it is a moot point anyway.

  - The elements of the quotient set are written $[g]$ (where g is any element of the relevant coset). For the present section we'll also write them explicitly as cosets gH. Depending on the context, we either mean an element of G/H or a subset of G.

- The obstruction to G/H being a group is that $gH \neq Hg$ in general. I.e., the condition for G/H to be a group is that $gH = Hg$ for all g. Equivalently, $gHg^{-1} = H$ for all g. If this holds, the cosets form a group. It also is the very condition under which the left and right partitions are the same and $G/H = H \setminus G$.

In fact, the condition is equivalent to requiring only that the *sets* of left and right cosets be the same (i.e. the left and right partitions be the same). This implies $gH = Hg$ for all g because $g \in gH$ and $g \in Hg$ so g must appear in the same class in both partitions and the two are the same.

- H is a **Normal Subgroup** if it obeys the conditions which make the cosets into a group.
  - We can refer to "cosets" instead of "left" or "right" cosets because the two are the same in this case.
  - A normal subgroup preserves cosets. I.e., $h(gH) = (gH)$ for all $h \in H$.

Pf: $gH = Hg$, so pick $h'g \in Hg$. Then $hh'g = (hh')g$. Since $hh' \in H$, $(hh')g \in Hg$. But $Hg = gH$, so $h(gH) \subseteq gH$. Suppose we pick an element of gH. Since $gH = Hg$, it can be written $h'g$ for some $h' \in H$. Let $x \equiv h^{-1}h'g \in Hg$ (and thus $x \in gH$). I.e., $hx = h'g$. So any element of $z \in gH$ has some element $x \in gH$ s.t. $hx = z$. I.e. $h(gH) \supseteq gH$ too, so we have $h(gH) = gH$.

  - Equivalently, N is normal in G iff $gNg^{-1} = N$ for all $g \in G$.

- Usually a normal subgroup is denoted N, and we write $N \triangleleft G$ (or $N \trianglelefteq G$).

- For a normal subgroup N, the Quotient Set $Q = G/N$ has (by definition) the natural structure of a group. It is called the **Quotient Group**.

What is the multiplication on Q? Denote by $[g]$ the coset gH. (i) The identity of G/N is $[e] = H$. (ii) If $k \in gH$, then $k = gh$ for some $h \in H$, so $k^{-1} = h^{-1}g^{-1}$. But $h^{-1} \in H$ so $k^{-1} \in Hg^{-1} = g^{-1}H$. Since this is true for every $k \in gH$, we have a meaningful $[g]^{-1} = [g^{-1}]$. (iii) Consider $k \in gH$ and $k' \in g'H$. Then $k = gh$ and $k' = g'h'$ for some $h, h' \in H$, so $kk' = ghg'h'$. But $hg' \in Hg' = g'H$ so $hg' = g'h''$ for some h''. I.e. $kk' = gg'h''h' \in (gg')H$. The cosets therefore multiply as expected. $[g][g'] = [gg']$. It is easy to show that the group axioms hold as well.

- We have two natural maps associated with a normal subgroup:
  - $N \xrightarrow{i} G$ is an inclusion (i.e. injection), defined by $h \to h$ (where the right-hand h is viewed in G).
  - $G \xrightarrow{q} Q$ is the quotient map (surjection), defined by $g \to gN$ (with the right-hand viewed as a coset, i.e. an element of G/N).

The injective homomorphism i is defined for any subgroup, not just normal ones.

The surjective map q is defined for any subgroup, with Q the quotient set. For normal subgroups, Q is a group and q is a homomorphism.

- By it's definition, N is a subgroup of G. Put another way, there is a copy of N in G. Though Q is a group derived from G and N and possesses no new info, there may or may not be a copy of it in G. Two natural questions are: (1) when is there a copy? and (2) how are G, N, and Q related in general? We'll address these shortly. In fact, doing so is the raison d'etre of these notes.

- What if we have more than one normal subgroup of G? Suppose we have $N_1 \triangleleft G$ and $N_2 \triangleleft G$.
  - The normal subgroups of G need not all be subgroups of one another. They form a lattice rather than a linear order.
  - It is quite possible for normal subgroups to be disjoint (in the group sense) or distinct-yet-isomorphic.
  - If $N_1 \approx N_2$, the resulting quotient groups need not be isomorphic in general.
    - If they are, N_1 and N_2 are called "series equivalent". The reason for this nomenclature will become clear shortly.

  * We'll shortly encounter a sufficient (but not necessary) condition for the quotient groups to be isomorphic. We'll also see that there can be some relatively unintuitive behaviors when it comes to series-equivalent normal subgroups.

- **Prop 2.1:** If G has two disjoint normal subgroups N_1, N_2 (in the sense that $N_1 \cap N_2 = \{e\}$), then N_1 and N_2 commute with one another.

Pf: Since N_1 and N_2 are normal, we know that $n_1 n_2 n_1^{-1} = n_2'$ for some $n_2 \in N_2$ and $n_2 n_1^{-1} n_2^{-1} = n_1'$ for some $n_1' \in N_1$. Now consider $n_1 n_2 n_1^{-1} n_2^{-1}$. This equals $(n_1 n_2 n_1^{-1}) n_2^{-1} = n_2' n_2^{-1} \in N_2$, but it also equals $n_1(n_2 n_1^{-1} n_2^{-1}) = n_1 n_1' \in N_1$. So it is in $N_1 \cap N_2 = \{e\}$. But if $n_1 n_2 n_1^{-1} n_2^{-1} = e$, then $n_1 n_2 = n_2 n_1$.

This doesn't imply that N_1 or N_2 commute internally, of course.

- **Prop 2.2:** Given G, $N \triangleleft G$, and subgroup $K \subset G$ (not necessarily normal) s.t. $N \cap K = \{e\}$, K has at most one element in each coset.

Pf: Suppose k, k' both are in the same coset. Then $k' \cdot k^{-1} \in N$, but K is a group so $k' \cdot k^{-1} \in K$ too. Since $N \cap K = \{e\}$, the only possibility is $k' = k$.

- **Prop 2.3:** If G has a normal subgroup N and a subgroup K (which need not be normal) s.t. N and K are disjoint (i.e. $N \cap K = \{e\}$) and $G = NK$ (i.e. every element of G can be written $g = nk$ for some $n \in N$ and $k \in K$), then:

  - (i) The decomposition $g = nk$ is unique.
  - (ii) Every coset gN in G/N contains a unique element of K.
  - (iii) Let $\pi_1 : G \to N$ and $\pi_2 : G \to K$ be the projection maps that take each g to its components (n and k in $g = nk$). Then $\pi_1|_N = Id_N$, $\pi_1(K) = e$, $\pi_2|_K = Id_K$, and $\pi_2(N) = e$.
  - (iv) π_1 and π_2 are surjective.
  - (v) π_2 is a homomorphism with ker $\pi_2 = N$.
  - (vi) $K \approx G/N$, and there is a unique isomorphism $\alpha_c : G/N \to K$ s.t. $\alpha_c \circ q|_K = Id_K$ (where q is the quotient map $G \to G/N$).
  - (vii) There is an injective homomorphism $K \to G$.
  - (viii) There is a surjective homomorphism $\tilde{q} : G \to K$ s.t. $\tilde{q}|_K = Id_K$.
  - (ix) K has a unique element in every coset of G/N.

Pf: (i) Suppose $g = nk$ and $g = n'k'$. Then $nk = n'k'$, so $n'^{-1}n = k'k^{-1}$. But $N \cap K = \{e\}$ so this is impossible.

Pf: (ii) Suppose k and k' are in the same coset. Then $k = k'n$ for some $n \in N$, which means $n = k'^{-1}k \in K$. But $N \cap K = \{e\}$ so this is impossible. Going the other way, consider coset gN. Any $g = nk$, but N and K commute, so this is kn, and $knN = kN$. I.e., all the g's in the coset have the same k and differ only in the choice of n.

Pf: (iii) Since there is a unique decomposition, $k = ek$ and $n = ne$, from which all four cases directly follow.

Pf: (iv) $\pi_1(N) = N$ and $\pi_2(K) = K$.

Pf: (v) Let $g_1 = n_1 k_1$ and $g_2 = n_2 k_2$. Then $\pi_2(g_1 g_2) = \pi_2(n_1 k_1 n_2 k_2)$. But N is normal, so its left and right cosets are equal and $k_1 n_2 = n_2' k_1$ for some $n_2' \in N$. Therefore, $\pi_2(n_1 n_2' k_1 k_2) = k_1 k_2$. Since $\pi_2(e) = e$ as well, it is a homomorphism. Note that the same does *not* hold for π_1 in general. To be in ker π_2 we need $g = ne$, which means $g \in N$.

Pf: (vi) We established that there exists a bijection between K and the cosets of G/N, which can be written $q|_K$. Since q is a homomorphism $G \to G/N$, it restricts to one on subgroup K. A bijective homomorphism is an isomorphism, so we can just define $\alpha_c([g]) \equiv q(\pi_2(g))$. This is well-defined because we established that $\pi_2(x)$ is the same for all members of a G/N coset, so it doesn't matter which representative g we use. Put another way, $\alpha_c^{-1} = q|_K$, which probably is the simpler way to define it in the first place.

Pf: (vii) This is just subset inclusion.

Pf: (viii) This is provided by π_2, which we saw is a surjective homomorphism and has $\pi_2|_K = Id_K$.

Pf: (ix) Since $q|_K$ defines an isomorphism $K \to G/N$, it is bijective from K to the cosets.

Note that we need the condition that every g can be written as nk solely for the infinite case. Because an infinite group can be isomorphic to a proper normal subgroup, we cannot guarantee that each coset contains an element of K otherwise. $q : G \to G/N$ is a surjective homomorphism which restricts to an injective homomorphism taking subgroup K to subgroup $q(K) \subset G/N$. Even if we had an isomorphism $\alpha : G/N \to K$, this only would give us an injective homomorphism $K \to K$ via $\alpha \circ q|_K$. For an infinite group this is entirely possible. We therefore have to explicitly postulate that each g has a decomposition into nk.

- **Prop 2.4:** Given group G, normal subgroup $N \triangleleft G$, and subgroup $K \subset G$ (which need not be normal), if $N \cap K = \{e\}$ and $q|_K$ is an isomorphism $K \to G/N$, then $G = NK$.

  I.e. given G, $N \triangleleft G$, and $K \subset G$ s.t. $N \cap K = \{e\}$ the conditions $G = NK$ and "$q|_K$ is an isomorphism" are equivalent. It follows that all of the results of Prop 2.3 hold if $N \cap K = \{e\}$ and $q|_K$ is an isomorphism.

  Pf: If $G = NK$, then Prop 2.3 tells us that $q|_K$ defines an isomorphism $K \to G/N$. Going the other way, we are told $q|_K$ is an isomorphism. Consider $k \equiv q|_K^{-1}(q(g))$. This picks out the representative element of the quotient-class for g. Trivially, $q(k) = q(g)$, so k and g are indeed in the same class. But this means $g = nk$ for some $n \in N$.

  Why can't we replace "$q|_K$ is an isomorphism" with the weaker condition $K \approx G/N$? Suppose $K \approx G/N$. Prop 2.2 tells us that since $N \cap K = \{e\}$, K has at most one element in each coset. I.e. $q|_K : K \to G/N$ is an injective homomorphism. $K \approx G/N$ implies a bijection between K and G/N. For finite G/N, this guarantees that every coset has one element of K, which means $q|_K$ must be surjective as well and thus an isomorphism. However, for infinite G/N, we have no such guarantee. It is quite possible to have a bijection between K and G/N, yet also have some cosets with no element of K. This is analogous to the fact that an infinite set can be bijective with a proper subset of itself. $q|_K$ is an isomorphism to some (infinite) subgroup of G/N, but this can be a proper subgroup. Note that the obstruction is the possible absence of an element of K from some cosets rather than the possible presence of multiple elements of K in the same coset. Prop 2.2 promises us the latter cannot happen.

- **Prop 2.5:** If the conditions of Prop 2.3 hold *and* K is normal (i.e. we're dealing with two normal subgroups N_1 and N_2) then we also have:

  - (i) N_1 and N_2 commute with one another.
  - (ii) Every coset gN_2 in G/N_2 contains a unique element of N_1.
  - (iii) $N_1 \approx G/N_2$, and there is a unique isomorphism $\beta_c : G/N_2 \to N_1$ s.t. $\beta_c \circ q'|_{N_1} = Id_{N_1}$ (where q' is the quotient map $G \to G/N_2$).
  - (iv) π_1 is a (surjective) homomorphism with ker $\pi_1 = N_2$.
  - (v) There is an injective homomorphism $N_1 \to G$.
  - (vi) There is a surjective homomorphism $\tilde{q'} : G \to N_1$ s.t. $\tilde{q'}|_{N_1} = Id_{N_1}$.

    Pf: (i) follows from Prop 2.1. The rest follow directly from Prop 2.3 by reversing the roles of the subgroups (since both now are normal). I.e. using $N = N_2$ and $K = N_1$.

2.2 Freeness and Transitivity of Group Action on Self

- There is a large and vibrant theory of group actions on sets, algebraic objects, and topological objects. For our purposes, we'll only care about the general notion.
- Here, $Aut(S)$ denotes whatever is the relevant automorphism group for S. I.e. bijections for sets, homeomorphisms for topological spaces, diffeomorphisms for manifolds, etc.

  Note that even if S has no group structure, $Aut(S)$ always is a group. This follows from the invertibility and composability of automorphisms of any type.
- **Action of Group G on S** (aka **left-action**): A homomorphism $\rho : G \to Aut(S)$.
- **Orbit of point $x \in S$** (under action ρ of G): The set of points $\rho_G(x)$. I.e. $\rho_g(x)$ for every $g \in G$. This is the set of points we can reach from x via the action of G.
- **Transitive action**: Given any $x, x' \in S$, there is some g s.t. $\rho_g(x) = x'$. I.e., we can get from any point to any other point via the action of G. Put another way, S consists of a single orbit under ρ.
- **Free action**: $\rho_g(x) = x$ iff $g = e$. I.e., every non-trivial g moves every point in S.
- **Left multiplication of G**: This is the action of G on itself (as the set $S = G$) via left-multiplication. I.e., $\rho_g(h) = g \cdot h$.

  There also is a right-action, defined in the obvious manner.
- **Prop 2.6:** Left-multiplication of G on itself is a free and transitive action.
- **Prop 2.7:** If $H \subset G$ is any subgroup, left-mult of G on itself induces an action of G on the quotient set G/H via $\rho_g([h]) \equiv [gh]$.

  Note that G/H is a set (and possibly a manifold if G is a Lie Group), but not a group unless $H \triangleleft G$.

2.3 Isomorphism Thms

Let's recall the "isomorphism theorems" for groups. Note that different people call these different things, and there is no uniform convention for the names.

- First Isomorphism Thm: Given any two groups G and H and a homomorphism $\phi : G \to H$, the following hold:
  - $\ker \phi$ is a normal subgroup of G
  - $\mathrm{Im}\ \phi$ is a subgroup of H
  - $\mathrm{Im}\ \phi$ is isomorphic to the quotient group $G/\ker \phi$.

    It follows that if ϕ is surjective then $H \approx G/\ker \phi$ as well.
  - Again, we have to ask: since $\ker \phi$ is a normal subgroup of G, and $\mathrm{Im}\ \phi$ is isomorphic to the quotient group $G/\ker \phi$ (which "sort of" may have an image in G), is it meaningful to write something like (playing fast and loose with notation) $G \overset{?}{=} \ker \phi \oplus \mathrm{Im}\ \phi$? The answer is no — it's more complicated. We'll discuss this shortly.
  - If ϕ is surjective, there is a natural isomorphism $H \approx G/\ker \phi$ which arises, so let's state it explicitly. It is $\alpha : G/\ker \phi \to H$ given by $\alpha([x]) \equiv \phi(x)$.

    Pf: This is well-defined because ϕ respects quotient classes. Let x' and x be in the same coset. Then $x' = xk$ for some $k \in \ker \phi$. This means $\phi(x') = \phi(xk) = \phi(x)\phi(k)$. But $\phi(k) = e$ since $k \in \ker \phi$. So $\phi(x') = \phi(x)$. To see that α is a homomorphism, we note that (i) $\alpha([e]) = \phi(e) = e$ and (ii) $\alpha([x][y]) = \alpha([xy])$ (by the group mult on $G/\ker \phi$) and $\alpha([xy]) = \phi(xy) = \phi(x)\phi(y) = \alpha([x])\alpha([y])$.
- Second Isomorphism Thm: Given any group G and subgroup $H \subseteq G$ and normal subgroup $N \trianglelefteq G$, the following hold:
  - HN is a subgroup of G (where HN is all products of elements).
  - $H \cap N$ is a normal subgroup of H.
  - $(HN)/N \approx H/(H \cap N)$.
  - Note that this does *not* imply $H \cap N$ is normal in G.

    This is a stronger condition because $gNg^{-1} \in N$ for all $g \in G$ not just all $g \in H$.
- Third Isomorphism Thm: Given any group G and subgroup $H \subseteq G$ and normal subgroup $N \triangleleft G$ s.t. $N \subseteq H \subseteq G$, the following hold:
  - H/N is isomorphic to a subgroup of G/N. If $H \triangleleft G$, then H/N is isomorphic to a normal subgroup of G/N.

    I.e., G/N effectively adds equiv classes to H/N rather than changing those in H/N.
  - Every subgroup of G/N is of this form for some subgroup H, and every normal subgroup of G/N is of this form for some normal subgroup H.
  - If $H \triangleleft G$, then $(G/N)/(H/N) \approx G/H$.
  - I.e. the set of subgroups containing N is bijective with the set of subgroups of G/N, and the set of normal subgroups containing N is bijective with the set of normal subgroups of G/N.
- Some useful properties of normal subgroups and quotient groups:
  - **Prop 2.8:** If $N \trianglelefteq G$ and $N \subseteq H \subseteq G$ (subgroups), then $N \trianglelefteq H$.

    Pf: If $gNg^{-1} \in N$ for all $g \in G$ then it holds for all $g \in H \subseteq G$.
  - Note that $H \triangleleft N$ and $N \triangleleft G$ do *not* imply $H \triangleleft G$. We do not have transitivity of normality.

    The dihedral group of order 8 is a counterexample.
  - **Prop 2.9:** If $f : G \to H$ is a surjective homomorphism, it preserves normality of subgroups. I.e., if $N \triangleleft G$ then $f(N) \triangleleft H$.

    Pf: Let $N \trianglelefteq G$. We want to show that for any $h \in H$ and $n \in N$, $hf(n)h^{-1} = f(n')$ for some $n' \in N$. This way $hf(N)h^{-1} = f(N)$. Since f is surjective, $h = f(g)$ for some g (it doesn't matter if g is not unique). Consider $f(gng^{-1}) = f(h)f(n)f(g)^{-1}$. Since N is normal in G, $\exists n'$ s.t. $gng^{-1} = n'$. So $f(h)f(n)f(g)^{-1} = f(n')$ and we are done. If f wasn't surjective, this wouldn't work of course.

- **Prop 2.10:** If $f : G \to H$ is a homomorphism and $N \triangleleft H$, then $f^{-1}(N) \triangleleft G$. Put simply, the inverse image of a normal subgroup is normal.

  > Bear in mind that f^{-1} is not a homomorphism in general. It is a one-to-many map unless f is injective.

  > Pf: Let $N \triangleleft H$. Define $K \equiv f^{-1}(N)$, and suppose it is not normal in G. Then $\exists g \in G, k \in K$ s.t. $gkg^{-1} \notin K$. This means $f(g)f(k)f(g^{-1}) \notin f(K) = N$. But $f(k) \in N$ and $f(g) \in H$ so we have $hnh^{-1} \notin N$ for some $n \in N$ and $h \in H$, which violates our assumption.

- Given $N \triangleleft G$, with quotient group $Q \equiv G/N$ with quotient map (i.e. projection) $q : G \to Q$, ker $q = N$.
- How do things map under homomorphisms? Let $f : G \to H$ be a homomorphism:
  - Subgroups are mapped to subgroups.
  - If f is surjective, normal subgroups are mapped to normal subgroups.
  - Let $N \triangleleft G$ and $M \triangleleft H$. Then f induces a homomorphism from G/N to H/M iff $f(M) \subseteq N$.

    > See `https://math.stackexchange.com/questions/3938314/group-homomorphism-between-quotient-groups` for a discussion.

- The normal subgroups of G are the kernels of homomorphisms from G to other groups.

  > This doesn't imply a bijection. Every normal subgroup is the kernel of at least one such homomorphism, and the kernel of any such homomorphism is a normal subgroup. However, there are many homomorphisms with the same kernel – so the map from homomorphisms to normal subgroups is surjective but not injective.

- The quotient groups of G (i.e. G/N for normal subgroups N) are the images of homomorphisms from G to other groups.

  > The same considerations hold as for normal subgroups and kernels. The map from homomorphisms to quotient groups is surjective but many-to-one. In fact, normal subgroups and quotient groups can be considered dual from a certain standpoint (from another category theory standpoint, quotient groups and general subgroups can be viewed as dual).

- I.e., the normal subgroups are kernels of homomorphisms and the quotient groups are images of homomorphisms.
- **Prop 2.11:** Given any homomorphism $f : G \to H$ and any $N \triangleleft G$ s.t. $N \subseteq \ker f$, there is an induced homomorphism $f' : G/N \to H$. I.e. under this condition f respects equivalence classes.

  > Pf: f is a surjective homomorphism to $f(G)$, so it gives rise to a normal/quotient relation of its own via $G/(\ker f)$. The corresponding cosets are of the form $g(\ker f)$. Clearly, f is constant on each since $f(gh) = f(g)f(h) = f(g)e = f(g)$ for $h \in \ker f$. But each coset $gN \subseteq g(\ker f)$, so each is contained in a coset of ker f and thus f is constant on it and respects the classes of G/N. This means it defines a homomorphism $f' : G/N \to H$ given by $f'([x]) = f(x)$, which we have seen is well-defined. Note that Im f' = Im f.

- **Prop 2.12:** Given groups G_1 and G_2, normal subgroups $N_1 \triangleleft G$ and $N_2 \triangleleft G_2$, and a homomorphism $f : G_1 \to G_2$ s.t. $f(N_1) \subseteq N_2$, there is a natural homomorphism $\tilde{f} : G_1/N_1 \to G_2/N_2$.
  - See `https://math.stackexchange.com/questions/36911/induced-homomorphism-by-passing-to-the-quotient` for a discussion.
  - Pf: By the first homomorphism thm, we have a surjective quotient homomorphism $q' : G_2 \to G_2/N_2$ with ker $q' = N_2$. Therefore, we have a (not-necessarily surjective) homomorphism $f^* : G_1 \to G_2/N_2$ given by $q' \circ f$. Since ker $q' = N_2$, ker $q' \circ f = f^{-1}(\ker q') = f^{-1}(N_2)$. Since $f(N_1) \subseteq N_2$, $N_1 \subseteq f^{-1}(N_2)$. I.e., $N_1 \subseteq \ker f^*$. By prop 2.11, this means f^* is class-respecting on G_1 and there is an induced map $\tilde{f} : G_1/N_1 \to G_2/N_2$ (what we called f' in prop 2.11) given by $\tilde{f}([x]) \equiv (q' \circ f)(x)$.
  - Intuitively, all that is being said is that the map f must respect classes on both ends — mapping all elements of a class in G_1/N_1 to a single class of G_2/N_2 (though it needn't do so surjectively). This is accomplished if $f(N_1) \subseteq N_2$ because then we are guaranteed to see cosets go to cosets.

2.4 Automorphisms and Isomorphisms

- Automorphisms can behave a little counterintuitively, so let's briefly consider some of their properties.

- Automorphisms need not preserve subgroups.

  - Like any homomorphism, an automorphism maps a subgroup to a subgroup — but it need not be the same subgroup.

- Put another way, an automorphism of G need not restrict to an automorphism of $H \subset G$.
- Suppose $f : G \to G$ is the automorphism. Then f takes a subgroup of G to a subgroup of G and f^{-1} does the same. Moreover, $f \circ f^{-1} = Id_G$. However, it is perfectly possible for f to take $H \subset G$ to $H' \subset G$ (and f^{-1} to take it back).
- As an example, consider $SO(3)$. Topologically, it is S^2. Great circles are subgroups corresponding to rotation around a given axis (i.e. they are copies of $SO(2)$). If we pick an axis and rotate the sphere around it, we take great circles into great circles, but (other than the unique great circle transverse to the axis) each great circle moves to a different one. I.e. $H \neq H'$.
- Given $f \in Aut(G)$, there are three things which can happen: (i) f takes subgroup H into a different subgroup H', (ii) f takes H into itself but moves elements around inside it (i.e. $f(H) = H$ overall), and (iii) H is fixed under f (i.e. $f(h) = h$ for all $h \in H$).
- In all cases, H is isomorphic to H' (with $f|_H$ the isomorphism).
- This carries over to normal subgroups. An automorphism maps normal subgroup N to isomorphic normal subgroup N', but we need not have $N = N'$ in general. Even if we do, the automorphism can move around elements within N (i.e. it can restrict to an automorphism on N rather than being Id_N).
- A subgroup $H \subset G$ for which every automorphism on G restricts to one on H is termed a "Characteristic Subgroup".

- Similarly, not every automorphism on H need extend to one on G. There may be automorphisms on H which are not the restriction of any automorphism on G.

- Note that when speaking of automorphisms, we should not confuse $f^{-1}(g)$ with $f(g)^{-1}$. For an ordinary isomorphism $f : G \to H$, there is no danger of confusion because $f^{-1}(g)$ has no meaning (since $f^{-1} : H \to G$). But for automorphisms it is possible to confuse the multiplicative inverse of an element with the inverse image under the automorphism. Only if f happens to take g to its inverse would the two be the same. Note that in general, the multiplicative-inverse map $g \to g^{-1}$ is *not* an automorphism because $(gh)^{-1} \neq g^{-1}h^{-1}$ but rather is $h^{-1}g^{-1}$. Only if G is abelian is it an automorphism.

- A few useful tips when proving maps are homomorphisms or isomorphisms:
  - To prove a map $f : G \to H$ is a homomorphism we need only prove that (i) $f(e) = e$ and (ii) $f(gh) = f(g)f(h)$.

    The fact that $f(g^{-1}) = f(g)^{-1}$ (again, multiplicative inverse, not fn inverse) follows because $f(gg^{-1}) = f(e) = e = f(g)f(g^{-1})$, and the same on the left.
  - To prove a map is an isomorphism we need only prove it is a bijective homomorphism.

    In fact, this commonly is taken as the definition of an isomorphism (as opposed to the existence of an inverse homomorphism). It is entirely equivalent.
  - If we have an *injective* homomorphism $f : G \to H$, then we have an isomorphism $f : G \to f(G) \subseteq H$.

- Some notes on group isomorphisms in general:
  - Two groups are isomorphic iff $\exists$ an isomorphism between them. However, there may be more than one such isomorphism. In a given situation, there may or may not be a natural choice of isomorphism. Even if one arises naturally, it may not be the isomorphism we care about.
  - This is most easily seen with $Aut(G)$. If there only was one isomorphism, $Aut(G)$ would be trivial.

    Although Id_G is a "natural" choice of automorphism, it is trivial and rarely what we care about.

    An an example we will encounter below, given two isomorphic normal subgroups $N \approx N'$ of G, we may care whether $\exists$ an automorphism of G which restricts to an isomorphism between N and N'. There may or may not be.
  - Warning: Given groups G and H, it is possible for there to be injective homomorphisms $G \to H$ and $H \to G$ but no isomorphism between G and H.

    This is in stark contrast to sets, where a pair of injective maps guarantees a bijection via the Schroder-Bernstein thm. For groups, the counterexamples necessarily are infinite. See https://math.stackexchange.com/questions/1259081/if-there-are-injective-homomorphisms-between-two-groups-in-both-directions-are for a discussion.

- **Prop 2.13:** If $G \approx H$, then
  - (i) $Aut(G) \approx Aut(H)$
  - (ii) Any specific isomorphism $\alpha : G \to H$ induces a specific isomorphism $\alpha^* : Aut(G) \to Aut(H)$ given by $\alpha^*(\gamma) \equiv \alpha \circ \gamma \circ \alpha^{-1}$.
  - (iii) $Iso(G, H)$ is bijective with $Aut(G)$ (and thus with $Aut(H)$).
  - (iv) Any two isomorphisms, $\alpha, \alpha' : G \to H$ are related by $\alpha' = \alpha \circ \gamma$ for a unique $\gamma \in Aut(G)$ and (equivalently) by $\alpha' = \beta \circ \alpha$ for a unique $\beta \in Aut(H)$.
  - Just as there may be no natural choice of isomorphism $G \to H$, there may be no natural choice of isomorphism $Aut(G) \to Aut(H)$.
  - Pf: (i,ii) Pick a specific isomorphism $\alpha : G \to H$. We define the isomorphism $\rho : Aut(G) \to Aut(H)$ via $\rho(\gamma) \equiv \alpha \circ \gamma \circ \alpha^{-1}$. This trivially is a homomorphism since $\rho(Id_G) = Id_H$ and $\rho(\gamma \circ \gamma') = \alpha \circ \gamma \circ \alpha^{-1} \circ \alpha \circ \gamma' \circ \alpha^{-1} = \rho(\gamma) \circ \rho(\gamma')$. I.e., it is a homomorphism due to the properties of invertible-function composition. We can use an identical argument to define $\rho'(\beta) \equiv \alpha^{-1} \circ \beta \circ \alpha$ as a homomorphism $Aut(H) \to Aut(G)$. Let's show they are inverses. $\rho'(\rho(\gamma)) = \alpha^{-1} \circ \alpha \circ \gamma \circ \alpha^{-1} \circ \alpha = \gamma$. A similar argument shows that $\rho(\rho'(\beta)) = \beta$. Note this proof depends heavily on the invertibility of α, β, and γ, so mere homomorphisms would not work. We've also exhibited the specific isomorphism needed for (ii). $\alpha^*(\gamma) \equiv \alpha \circ \gamma \circ \alpha^{-1}$.
  - Pf: (iii) Pick any fixed isomorphism $\alpha : G \to H$. Given any $\gamma \in Aut(G)$, we have a unique $\alpha' : G \to H$ given by $\alpha \circ \gamma$. Why is it unique? Suppose $\alpha \circ \gamma = \alpha \circ \gamma'$. Since γ and α both are invertible, we could compose α^{-1} on the left and γ^{-1} on the right to get $\gamma' \circ \gamma^{-1} = Id_G$. $Aut(G)$ is a group, so each element has a unique inverse. We thus have an injective map (dependent on our choice of α, of course) from $Aut(G)$ to $Iso(G, H)$, which we'll call ρ_α (i.e. $\rho_\alpha(\gamma) \equiv \alpha \circ \gamma$). Let's show it's surjective as well. Given any isomorphism $\alpha' : G \to H$, we need a $\gamma \in Aut(G)$ s.t. $\alpha' = \alpha \circ \gamma$. I.e., $\alpha' \in \rho_\alpha(Aut(G))$. Compose α^{-1} on the left to get $\gamma = \alpha^{-1} \circ \alpha'$. We thus have surjectivity, and our map is a bijection. Note that $Iso(G, H)$ is not a group and ρ_α is *not* a homomorphism.
  - Pf: (iv) Along similar lines, suppose we have isomorphisms $\alpha, \alpha' : G \to H$. Define $\gamma \equiv \alpha^{-1} \circ \alpha'$. Then $\gamma \in Aut(G)$ and $\alpha' = \alpha \circ \gamma$. Note that we could just as well have done it the other way to get α from α' using the automorphism $\gamma^{-1} = \alpha'^{-1} \circ \alpha$. On the other end, if we define $\beta \equiv \alpha' \circ \alpha^{-1}$ then $\alpha' = \beta \circ \alpha$. Again, we equally well could have written $\alpha = \beta^{-1} \circ \alpha'$.

2.5 Uniqueness of normal and quotient groups

- **Prop 2.14:** Given G, there is a canonical bijection between the set of normal subgroups and set of quotient groups. I.e., each normal subgroup defines a unique quotient group, and no $G/N = G/N'$ for $N \neq N'$.

  Pf: Given N, G/N is the group of cosets of N in G — so by construction it is unique. Moreover, $[e] = N$, so it cannot be the quotient of any other N' or we would need $N = N'$.

  Note that we have to be a bit careful here. We should not confuse this with the fact that an automorphism of N doesn't necessarily induce one on G or G/N. It is quite possible to have an automorphism $N \to N$ which does not extend to one on G, in which case the resulting G/N may not map to itself automorphically either. However, that is a question of how things transform. Here, we are simply asking whether the quotient group is unique. N is a particular subgroup and G/N is a particular group derived from it. So yes, it is.
- This speaks to exact equality, but what about isomorphism? Let's now consider this.
- Suppose N and N' are normal subgroups of G and $N \approx N'$. In general, the quotients need not be isomorphic. I.e. $G/N \not\approx G/N'$. However, we have the following case where the quotients always are isomorphic.
- **Prop 2.15:** If $N \triangleleft G$ and $N' \triangleleft G$ and $N \approx N'$ via some isomorphism $h : N \to N'$ which extends to an automorphism on G, then $G/N \approx G/N'$.
  - I.e. if $\exists \alpha \in Aut(G)$ s.t. $\alpha|_N$ is an isomorphism $N \to N'$, then $G/N \approx G/N'$.
  - Put another way, in this case N and N' are series-equivalent.
  - Pf: Suppose $N \triangleleft G$ and $N' \triangleleft G$ and $N \approx N'$ via some isomorphism $h : N \to N'$. A coset of N is gN, and $h(gN) = h(g)h(N) = h(g)N'$ is a coset of N'. The same holds the other way using h^{-1}. So we have a bijection between cosets of N and those of N' (i.e. a bijection between G/N and G/N'). This map $k : G/N \to G/N'$ is defined as $k([g]) \equiv [h(g)]'$ (where $[g] = gN$ is a coset of N and $[g]' = gN'$ is a coset of N'). The homomorphism properties of h then carry over to k. Since $h(e) = e$, $k([e]) = [e]'$ and since $h(g^{-1}) = h(g)^{-1}$, $k([g]^{-1}) = k([g^{-1}]) = [h(g^{-1})]' = [h(g)^{-1}]' = [h(g)]'^{-1}$. Similarly, $h(gg') = h(g)h(g')$ implies $k([g][g']) = k([gg']) = [h(gg')]' = [h(g)h(g')]' = [h(g)]'[h(g')]'$. As a bijective homomorphism, k is an isomorphism. So $Q \approx Q'$. Note why we needed h to be the restriction of an automorphism of G rather than just an isomorphism $N \to N'$. We must apply h to arbitrary $g \in G$, not just $h \in H$. Similarly, it couldn't just be a homomorphism $G \to G$ that happens to restrict to an isomorphism $N \to N'$ because we need the same to hold of its inverse.

  - This is the sufficient (but not necessary) condition alluded to earlier for the quotients to be isomorphic.
  - It is quite possible to have isomorphic normal subgroups but no G-automorphism which maps them to one another. In that case, the condition for this result is violated and G/N may or may not be isomorphic to G/N'.
  - As we will see when discussing short exact sequences, the "not-necessary" part can give rise to some unintuitive situations. The cases where no such extension exists yet N_1 and N_2 are series-equivalent are termed "series-equivalent non-automorphic", and we'll have more to say about them later.
  - See https://math.stackexchange.com/questions/40881/isomorphic-quotients-by-isomorphic-normal-subgroups and https://groupprops.subwiki.org/wiki/Series-equivalent_not_implies_automorphic for some examples.

- It also is possible to have isomorphic quotient groups without having isomorphic normal subgroups.

  See https://math.stackexchange.com/questions/40881/isomorphic-quotients-by-isomorphic-normal-subgroups and https://math.stackexchange.com/questions/1584568/isomorphic-quotient-groups-fracgh-cong-fracgk-imply-h-cong-k and https://math.stackexchange.com/questions/40763/isomorphic-quotient-groups/ for a detailed discussion of various situations and some examples.

- In summary, the following unintuitive situations can arise:
  - $N_1 \approx N_2$ but $G/N_1 \not\approx G/N_2$.
  - $N_1 \not\approx N_2$ but $G/N_1 \approx G/N_2$.
  - $N_1 \approx N_2$ and $G/N_1 \approx G/N_2$ but no automorphism on G takes N_1 to N_2.

2.6 Similar concepts

Normal subgroups should not be confused with certain similar concepts:

- The **center of group** G is the set of all elements which commute with the entirety of G. It is a normal subgroup and typically is denoted $Z(G)$.
  - Obviously, $Z(G)$ is abelian.
  - Note that other normal subgroups of G need not be in the center. Normality requires that $ghg^{-1} \in N$ for all $g \in G$ and $h \in N$, whereas $Z(G)$ requires that $gzg^{-1} = z$ for all $g \in G$ and $z \in Z(G)$. Put another way, N commutes with G set-wise but not at the level of individual elements, whereas $Z(G)$ commutes with G at the level of individual elements.
  - The center is *not* a functor from GRP to AB, because it is not preserved by homomorphisms.
  - $Z(G) = G$ iff G is abelian.
  - If $Z(G)$ is trivial, then no nonidentity element commutes with all of G.
  - **Prop 2.16:** If $H \subset G$, then $(Z(G) \cap H) \subseteq Z(H)$.

    Pf: Suppose $x \in Z(G) \cap H$ (i.e. it's an element of H in $Z(G)$). Then it commutes with all of G and thus H too. So $x \in Z(G) \cap H$ implies $x \in Z(H)$. However, it is possible to have $x \in H$ which commutes with all of H but fails to commute with all of G. In that case, $x \in Z(H)$ but $x \notin Z(G) \cap H$.

- The **commutator of two elements of** G is $[g,h] \equiv g^{-1}h^{-1}gh$.
  - Obviously, it is e iff g and h commute.
  - Also, $[g,h] = [h,g]^{-1}$.
  - This should not be confused with the commutator in a matrix-based Lie Algebra, which is $[x_1, x_2] = x_1x_2 - x_2x_1$. There, we define the bracket in terms of the associative multiplication of matrices, and subtraction is part of the the vector-space structure. For groups, we have a single operation and no notion of subtraction.

- The **commutator subgroup of** G is the subgroup of G generated by all its commutators.
  - Denoted $[G,G]$.
  - Note that G isn't just the set of commutators. It is *generated* by that set. I.e., it consists of all products of commutators. The inverses are included automatically, because $[g,h] = [h,g]^{-1}$.

- $[G, G]$ is a normal subgroup of G.
- $[G, G]$ is preserved by homomorphisms (most notably, automorphisms) and defines an endofunctor on GRP.
- In general, $[G, G]$ is not abelian (and thus is not a subgroup of $Z(G)$).
- $[G, G]$ is trivial iff G is abelian.
- If $[G, G] = G$, it does *not* mean that no two (non-identity) elements of G commute. This just means that every element of G appears as the product of commutators of some pairs of elements.

  Equivalently, it means that G can be generated from some set of commutators of elements.
- **Perfect Group**: Satisfies $[G, G] = G$. In a sense, a perfect group is maximally non-abelian.

- The **abelianization of group** G is the quotient group $G/[G, G]$.
  - It is a group because $[G, G] \triangleleft G$, but it need not be isomorphic to a subgroup of G.
  - $G/[G, G]$ is abelian.
  - It is preserved by homomorphisms, and thus defines a functor from GRP to AB.

    This turns out to be the free construction going from GRP to AB and is the left adjoint of the inclusion functor from AB to GRP (which is just the corresponding forgetful functor).
  - Basically, the quotient removes all nontrivial commutators by assigning them to identity.
  - $G/[G, G]$ is trivial iff G is a perfect group (i.e. $[G, G] = G$).
  - $G/[G, G] = G$ iff G is abelian (in which case $[G, G]$ is trivial).
  - Again, the abelianization is *not* necessarily isomorphic to a subgroup of G. Even if it happens to be, it need not be isomorphic to a normal subgroup. Put another way (in language we have yet to discuss), the SES $e \rightarrow [G, G] \xrightarrow{i} G \xrightarrow{q} G/[G, G] \rightarrow e$ need not right-split, let alone left-split.

- Some notes:
  - A group G may have many normal subgroups but it always has a unique center $Z(G)$, commutator subgroup $[G, G]$, and abelianization $G/[G, G]$.

    Of course, any of these may equal G or be trivial.
  - For an abelian group: $Z(G) = G$ and $G/[G, G] = G$ and $[G, G] = \{e\}$.
  - For a perfect group: $Z(G) = \{e\}$ and $G/[G, G] = \{e\}$ and $[G, G] = G$.
  - A subgroup of G can be abelian without being in the center or even normal.

    To be abelian, we only need $[h_1, h_2] = e$ for all $h_1, h_2 \in H$. I.e., $[H, H] = e$. To be in the center, we need $[G, H] = e$. To be normal, we need $gHg^{-1} \in H$ for all $g \in G$, but the fact that H commutes with itself doesn't give us that.

    Ex. consider $SO(3)$, the group of rotations in $3D$. It is nonabelian, but $SO(2) \subset SO(3)$ is abelian (we can pick this subgroup in many ways, corresponding to a choice of axis of rotation, but it doesn't matter which we choose). $SO(3)$ has no nontrivial proper normal subgroups, so $SO(2)$ is not normal in it. $SO(2)$ also doesn't commute with it, so it isn't in the center.

2.7 Inner and Outer Automorphisms

These notions only will be used in the addendum where we explicitly construct group multiplication for a group extension. They may be skipped if those details are not of interest to the reader.

- Given a group G, we have the group $Aut(G)$ of its automorphisms. These may be divided into inner and outer automorphisms via a normal/quotient relationship of their own.

- **Inner automorphism of G:** Any automorphism of the form $h \to ghg^{-1}$ for some fixed $g \in G$ (and all $h \in G$). I.e., a conjugacy automorphism $G \to gGg^{-1}$.
  - The inner automorphism gGg^{-1} usually will be denoted $\phi_g : G \to G$.
  - The set of these is denoted $Inn(G)$.
  - $Inn(G)$ is a subgroup of $Aut(G)$.

    Pf: Multiplication on $Aut(G)$ is composition. For inner automorphisms, $\phi_{gg'}(h) = gg'h(gg')^{-1} = gg'hg'^{-1}g^{-1} = \phi_g(\phi_{g'}(h))$. Also, $Id_G = \phi_e$ so $Inn(G)$ contains the identity.
  - $Inn(G)$ is normal in $Aut(G)$.

    Pf: Let $\alpha \in Aut(G)$. $(\alpha \circ \phi_g \circ \alpha^{-1})(h) = \alpha(g\alpha^{-1}(h)g^{-1}) = \alpha(g)\alpha(\alpha^{-1}(h))\alpha(g^{-1}) = \alpha(g)h(\alpha(g))^{-1}$ which is of the form $g'hg'^{-1}$ and thus a conjugacy automorphism. Note that $(\alpha(g))^{-1}$ is the multiplicative inverse element in G of $\alpha(g)$. It is not to be confused with $\alpha^{-1}(g)$, which denotes the inverse automorphism applied to g.
  - $\phi_g(h)$ commonly is written ${}^gh$ as well. We won't use this notation.
  - Some people use $g^{-1}hg$ and h^g instead. This is entirely equivalent, though the individual elements of $Inn(G)$ then would be labeled differently.
  - $Inn(G)$ kind of measures the failure of G to commute.
    - **Prop 2.17:** G is abelian iff $Inn(G)$ is trivial.
  - **Prop 2.18:** $\phi \in Aut(H)$ is inner iff it extends to an inner automorphism on all groups containing H.
    - I.e., if $H \subset G$ and $\phi \in Inn(H)$ then $\phi \in Inn(G)$.
    - Put another way, inner automorphisms remain inner if we grow the group.

- **Outer automorphism group $Out(G)$:** The quotient group $Out(G) \equiv Aut(G)/Inn(G)$.
  - Note that the term "Outer automorphism" itself can be used in two ways. It could be an element of $Out(G)$, which is a class of automorphisms rather than an individual automorphism. We less commonly care about $Aut(G) - Inn(G)$, but some people use "outer automorphism" to refer to an element of this instead (i.e., any automorphism which is not inner).
  - As with any other quotient, $Aut(G)$ could be a direct sum, semidirect product, or general group extension of $Out(G)$ by $Inn(G)$.

    The purpose of these notes is to develop these very notions, so don't worry about them now. This just is an observation for future reference.

- **Prop 2.19:** There is a natural surjective homomorphism $\phi : G \to Inn(G)$ given by $g \to \phi_g$.

  Pf: $\phi_e(a) = a$ so $\phi_e = Id_G$ and the identity is preserved. $\phi_{gg'}(h) = gg'hg'^{-1}g^{-1} = \phi_g(\phi_{g'}h)$ and multiplication is honored. Surjective follows from the definition of $Inn(G)$.

  Why isn't ϕ an isomorphism? The only culprit could be a failure of injectivity. Is it possible that $\phi_g = \phi_{g'}$ for $g \neq g'$? Yes. For example, any element $x \in Z(G)$ commutes with all of G, so $\phi_x = \phi_e$. As we will see shortly, this is the only obstruction. If $Z(G) = e$ then $G \approx Inn(G)$.

- **Prop 2.20:** An inner automorphism ϕ_h equals Id_G iff $h \in Z(G)$.
  - I.e., ker $\phi = Z(G)$, where ϕ is the homomorphism $G \to Inn(G)$ in prop 2.19.
  - Pf: If $h \in Z(G)$, then it commutes with G so we get Id_G. If $\phi_h = Id_G$, then $hgh^{-1} = g$ for every $g \in G$. I.e., h commutes with every element and thus is in $Z(G)$.

- **Prop 2.21:** $Inn(G) \approx G/Z(G)$.

  Pf: We have a surjective homomorphism $\phi : G \to Inn(G)$ with ker $\phi = Z(G)$. The first homomorphism thm tells us $Inn(G) \approx G/Z(G)$.
  - Cor: If $Z(G) = e$ then $Inn(G) \approx G$.
  - Cor: If G is abelian, $Inn(G)$ is trivial.

- **Prop 2.22:** If $H \subset G$, then $Inn(H)$ is isomorphic to a subgroup of $Inn(G)$.

  Pf: There's an injective homomorphism $Inn(H) \to Inn(G)$ given by $\phi_{h \in H} \to \phi_{h \in G}$. Why is it injective? If ϕ_h and $\phi_{h'}$ are distinct inner automorphisms of H, then they remain distinct when extended to all of G. Even if they don't differ on the rest of G, they still must on $H \subset G$.

- Let $H \subset G$. There are several obvious ways to restrict things to H:
  - 1. We can restrict a general automorphism f of G to $f|_H$ on H. However, $f|_H$ is not necessarily an automorphism of H. I.e., automorphisms of G do not necessarily restrict to automorphisms on H.

    f need not map H to itself. It could map it to a subgroup of itself (if H is infinite) or to some other isomorphic subgroup of G.

  - 2. We can restrict an inner automorphism on G to H. I.e., we apply ϕ_g only to H (but allowing $g \in G$). In general, this does not yield an automorphism of H for the same reason as above. For a normal subgroup $N \triangleleft G$, it *does* yield an automorphism of N but not necessarily an inner automorphism of N.

    Pf: ϕ_g conjugates N by an element of g and thus takes N to N (though it can move elements around within N, of course). As such, it produces an automorphism of N. However, an inner automorphism of N requires conjugation by an element of N itself. There may be no $n \in N$ s.t. $(\phi_n)|_N = (\phi_g)|_N$.

  - 3. We can consider the subgroup of $Inn(G)$ consisting of conjugacy by elements of H (though still viewed as automorphisms on G). We'll denote this $Inn_H(G) \subset Inn(G)$. Each such element clearly restricts to an inner automorphism of H as well. In fact, $Inn_H(G)|_H = Inn(H))$.
  - **Prop 2.23:** $Inn(H) \approx Inn_H(G)$ iff $(Z(G) \cap H) = Z(H)$. However, we always have a surjective homomorphism $Inn_H(G) \to Inn(H)$.

    Pf: Let ϕ'_h denote an element of $Inn(H)$ and let ϕ_h denote an element of $Inn_H(G)$. The map $f : Inn_H(G) \to Inn(H)$ given by $f(\phi_h) \equiv \phi'_h$ is a surjective homomorphism. To see this note that ϕ'_h is just the restriction of ϕ_h to H. Since $f(\phi_e) = \phi'_e = Id_G$ and $f(\phi_h \circ \phi_{h'}) = f(\phi_{hh'}) = \phi'_{hh'} = \phi'_h \circ \phi'_{h'}$, we have a homomorphism. Surjectivity of f is trivial. This is just a pedantic demonstration of the obvious relationship: the restriction of $Inn_H(G)$ to H. However, f is not injective in general. It is possible that two elements of $Inn_H(G)$ differ on their action outside of H but not on their action within H. Suppose $\phi'_h = \phi'_{h'}$ for some $h \neq h'$. Then $\phi'_{hh'^{-1}} = Id_H$, which means hh'^{-1} commutes with H. Since $h \neq h'$ by assumption, $hh'^{-1} \neq e$ and $Z(H)$ is nontrivial. Conversely, if $x \in Z(H)$ then pick any h and let $h' = xh$ (which can't equal h). I.e. $hh'^{-1} \in Z(H)$. Then $\phi'_h \circ \phi'_{h'^{-1}} = \phi'_e = Id_H$, so $\phi'_h = {\phi'_{h'^{-1}}}^{-1}$. Because ϕ' is a homomorphism $H \to Inn(H)$, ${\phi'_h}^{-1} = \phi'_{h^{-1}}$ (since $\phi'_h \circ \phi'_{h^{-1}} = \phi'_{hh^{-1}} = \phi'_e = Id_H$). So $\phi'_h = \phi'_{h'}$. We thus have shown that $\phi'_h = \phi'_{h'}$ iff $hh'^{-1} \in Z(H)$. Similarly, $\phi_h = \phi_{h'}$ on G iff $hh'^{-1} \in Z(G) \cap H$. I.e., we can have $\phi_h \neq \phi_{h'}$ on G but $\phi'_h = \phi'_{h'}$ on H iff $hh'^{-1} \in (Z(H) - (Z(G) \cap H))$. This is the situation in which injectivity fails, because ϕ_h and $\phi_{h'}$ are distinct but ϕ'_h and $\phi'_{h'}$ are not. f therefore is an isomorphism (bijective homomorphism) iff $Z(H) = Z(G) \cap H$. If it's not, all we have is a surjective homomorphism $f : Inn_H(G) \to Inn(H)$.

  - We saw that not every automorphism of G restricts to an automorphism of $H \subset G$ (or even on $N \triangleleft G$). However, we also saw that every inner automorphism of $N \triangleleft G$ is the restriction of (at least) one on G. It is natural to ask whether every general automorphism of $H \subset G$ (or perhaps of $N \triangleleft G$) extends to an automorphism of G. The answer in both cases is no. There may be automorphisms on H (even if normal) which are not the restriction of any automorphism of G.
  - I.e., G can have automorphisms which don't restrict to automorphisms on H and H may have automorphisms which don't extend to automorphisms on G.

- **Prop 2.24:** Inner automorphisms preserve normal subgroups.

  Pf: An automorphism maps normal subgroup $N \subset G$ to isomorphic normal subgroup $N' \subset G$, though N need not equal N' in general. But an inner automorphism ϕ_g is just conjugation by g, and conjugation preserves a normal subgroup N (though it may move elements within it, of course).

- **Prop 2.25:** If $N \triangleleft G$, there is a natural homomorphism $\alpha : Inn(G) \to Aut(N)$ given by $\alpha(f) = f|_N$.
  - Pf: We saw this before. Every inner automorphism of G restricts to an automorphism of N. The fact that α is a homomorphism follows trivially from composition.
  - α restricts to the isomorphism (or equality, depending how we wish to write it) $Inn_H(G) \approx Inn(H)$ when confined to $Inn_H(G)$ as its domain.

- **Prop 2.26:** If $N \triangleleft G$, there is a natural homomorphism $G \to Aut(N)$.

  Pf: We saw there is a natural surjective homomorphism $\phi : G \to Inn(G)$ taking g to ϕ_g. We also have a natural homomorphism $\alpha : Inn(G) \to Aut(N)$ given by $\alpha(\phi_g) = (\phi_g)|_N$. Composition gives us a (not necessarily surjective) homomorphism $\alpha \circ \phi$.

- **Prop 2.27:** Given $N \triangleleft G$, we have a natural homomorphism $\beta : G/N \to Out(N)$.

  Pf: As seen above, we have a homomorphism $\gamma : G \to Aut(N)$ given by $\gamma(g) = (\phi_g)|_N$. We also have a surjective homomorphism $f : Inn_N(G) \to Inn(N)$. Note that γ gives us a natural way to twist N by moving around all of G, but that is too much freedom. A general homomorphism $G \to Aut(N)$ won't respect the quotient classes. I.e., we need that $\gamma(x) = \gamma(x')$ (as automorphisms) when $g(x) = g(x')$. Back to the proof, we are given (i) that $N \triangleleft G$ and (ii) we know that $Inn(N) \triangleleft Aut(N)$, and (iii) we have a homomorphism $\gamma : G \to Aut(N)$, and (iv) $\gamma(N) = Inn(N)$ because each n maps to the inner automorphism $n \to nn'n^{-1}$ (the map may not be injective, but that is fine). These are the conditions for Prop 2.12. So we have an induced homomorphism $f' : G/N \to Aut(N)/Inn(N)$ given by $f'([x]) = [\phi'_x]$ (where $\phi'_x(n) \equiv xnx^{-1}$). However, $Out(N) \equiv Aut(N)/Inn(N)$, so we have the homomorphism $\beta = f'$.

  How do we interpret this? γ maps $x \in G$ to the inner automorphism ϕ_g on G. This restricts to an automorphism of N. Because $Inn(N)$ is normal in $Aut(N)$, $\phi_g|_N = f\phi'_n$ for some $n \in N$ and $f \in Aut(N)$ (of course, there are many ways to choose the f, n pair). We thus have a map from each g to ϕ_g to the class of all f's s.t. $\phi_g|_N = f\phi'_n$ for some n. If we start with $\gamma(n \in N) = \phi_n$ then we get $\phi_n|_N = Id_N\phi'_n$ along with many other $f\phi'_{n'}$'s. But these all sit in $[Inn(N)] = [e]$, since their class contains $Id_N = \phi'_e$. So we have $\gamma(N) \subseteq Inn(N)$. The resulting map takes each class of G to the corresponding class of restricted (to N) inner automorphisms on G modulo actual inner automorphisms on N.

3 Exact Sequences

3.1 Definitions

An **exact sequence** is a sequence of homomorphisms between groups $\cdots \to G_n \xrightarrow{f_n} G_{n-1} \xrightarrow{f_{n-1}} \cdots$ where Im $f_n = \ker f_{n-1}$ for every pair. Here are some basic properties:

- $e \to A \xrightarrow{f} B \cdots$ says f is injective.
- $\cdots A \xrightarrow{f} B \to e$ says f is surjective.
- $e \to A \to B \to e$ says $A \approx B$.

A **short exact sequence (SES)** is an exact sequence of the form: $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$. From now on, almost everything we discuss will involve SES's.

- For an SES, f is injective, g is surjective, and Im $f = \ker g$.

- **Prop 3.1:** Given an SES, (i) $f(A)$ is normal in B, (ii) $C \approx B/f(A)$ is a group, and (iii) there is an isomorphism $\alpha : B/f(A) \to C$ given by $\alpha([x]) \equiv g(x)$ (which is well-defined).

  Pf: This immediately follows from the first isomorphism thm applied to the groups at hand. g is a surjective homomorphism, so ker g is normal in B and $C \approx B/f(A)$ is a group. Since ker g = Im f, $f(A)$ is normal in B. Likewise, α is the natural isomorphism discussed earlier.

- Because A is injective, it is common to just refer to A rather than $f(A)$ as the subgroup of B. In that case, the choice of f is implicit but important. Though in many cases, there is a natural choice (such as an inclusion when A truly *is* a subgroup of B), it is quite possible that there exists more than one subgroup of B isomorphic to A. In that case, different f's would give different SES's. As we will see, these correspond to distinct group extensions.

- SES's arise all the time when dealing with groups, and the critical question is whether they "split".

  As suggested in Prop 3.1 and developed below, an SES embodies a normal/quotient relationship between groups (with a little extra sugar). The most general form of this is a group extension. If the SES right-splits we get a semidirect product, and if it left-splits we get the direct sum.

- Note that sometimes the e's (or 0's or 1's) are omitted from the ends of an SES. In that case, whether the expression is indeed an SES should be clear from the context.

An SES is said to **right-split** if $\exists$ a homomorphism $h : C \to B$ such that $g \circ h = Id_C$.

- Obviously, this implies h is injective.

  Otherwise, two elements could map to the same b. g then would map them to the same c on round-trip, and $g \circ h \neq Id_C$.

- I.e. we have a full copy of C inside B, which means C is (isomorphic to) a subgroup of B.

  - Technically, C is isomorphic to a subgroup of B, but just as it is common to treat A (rather than $f(A)$) as a subgroup of B for an SES in general, it is common to treat C (rather than $h(C)$) as a subgroup of B when the SES right-splits. In this case, the choice of h is implicit. In a given case, there may be a natural choice of h. But if not, distinct h's will give rise to distinct ways of splitting the SES. As we will see, these correspond to distinct semidirect products.
  - One way of thinking of this is as follows. g projects all of B to C. This is done in a manner compatible with the quotient map $q : B \to B/f(A)$, producing the isomorphism $\alpha : B/f(A) \to C$ we mentioned earlier (i.e. $\alpha([x]) = g(x)$). If the SES right-splits then we can reconstitute $B/f(A)$ as a subgroup of B by picking one element from each equivalence class via $h \circ \alpha : B/f(a) \to B$.
  - Note that for *any* SES, we always can pick an element from each class of $B/f(A)$ (and thus from $\alpha(B/f(a)) \in C$). This produces an injective map $B/f(A) \to B$. However, this map need not be a homomorphism. It may be impossible to choose an element from each class in a way that respects the group structure on $B/f(A)$ (and thus on C). I.e., we can construct many injective maps h s.t. $g \circ h = Id_C$, but none of them need be a homomorphism. If any are, the SES right-splits.
  - Given that every SES has the canonical isomorphism $\alpha : B/f(A) \to C$ described above, why not just use α^{-1} to obtain a right-splitting map? α^{-1} takes us from C to $B/f(A)$. The only way to go to B is if there is an injective homomorphism $B/f(A) \to B$ to compose on this — which is precisely the case when the SES right-splits. The freedom to pick that injective homomorphism is the freedom in the right-splitting map.

- If an SES right-splits, there may be more than one way to do so. "right-splitting" (i.e. whether *any* suitable homomorphism h exists) is a property of the SES, but a specific "right-split" SES involves a choice of h.

An SES is said to **left-split** if $\exists$ a homomorphism $h : B \to A$ such that $h \circ f = Id_A$.

- Obviously, this implies h is surjective.

- We always can move from A to B and back without losing info, because f is an injective homomorphism. However, this only applies to the round-trip through Im $f \subseteq B$. We have no way of projecting all of B to A, since f^{-1} is not defined on all of B. h fills this gap. Its domain is all of B, not just Im f. Also, it is surjective (otherwise, it couldn't compose to produce Id_A). I.e., if we write it as $B \underset{f}{\overset{h}{\rightleftarrows}} A$, this looks like the right-half of a right-split SES. We're projecting B to A in such a way that A looks like a quotient group. The presence of h gives us the ability to do so.

- Another way to phrase this is that f^{-1} is defined only on $f(A)$, and h extends it to a homomorphism from all of B to A. I.e., the SES left-splits iff f^{-1} extends (as a homomorphism) to all of B. Equivalently, the SES left-splits iff $\exists$ a homomorphism $B \to A$ that restricts to f^{-1} on $f(A)$.

- As with right-splitting, left-splitting (i.e. whether any suitable h exists) is a property of the SES, but a specific left-split SES involves a choice of h.

  However, in the case of left-splitting, the choice of h is far less meaningful. As we will see, this is because it is such a strict condition. A left-split SES corresponds to a direct sum of groups and this is a unique construction.

- Left-splitting is a far stronger constraint than right-splitting, and in fact implies it.

  The directionality of the homomorphisms in the SES introduces this asymmetry of information content.

  If the groups are abelian, the converse holds too and right-splitting implies left-splitting.

- Another way to think of it is that a left-split SES can be reversed using the appropriate h's in place of f and g.

- Different people use the unadorned term "splitting" to refer to right-splitting or left-splitting, so it is best to include the specific moniker.

3.2 Central Extensions

- **Central Extension** of C by A: An SES $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$ for which $f(A) \subseteq Z(B)$.

  - I.e., A injects into the center of B.
  - This means $f(A)$ is both abelian and normal in B.
  - Note that sometimes A or f themselves are referred to as the "central extension".

    The reason for the nomenclature will become apparent later, when we equate SES's with group extensions.
  - This implies A itself is abelian.

    Pf: A is isomorphic to $f(A)$ since f is an injective homomorphism. However, $f(A) \subseteq Z(B)$ is abelian. So any group isomorphic to $f(A)$ must be abelian as well.
  - The converse need not hold. A can be abelian without being a central extension.

    $f(A)$ can commute with itself but fail to commute with the rest of B.

- Given any group C and any abelian group A, we always can construct a central extension.

  Pf: As we'll discuss later, we always can build $B = A \oplus C$. The inclusion is $f : A \to (A, e)$, which clearly is in $Z(B)$.

  This does not contradict our previous statement. Given C and abelian A, there may exist non-central-extension SES's. However, there always exists a central extension as well.
- Central extensions play a critical role in projective representations and quantum mechanics.

  More on this another time, but here's the gist. Quantum mechanics has a projective Hilbert space as its true state space, but we mostly work in the far more tractable corresponding Hilbert space. One of the main reasons we can do so is because the projective representations of a symmetry group G (i.e. the angle-preserving actions of G on projective Hilbert space) can be "lifted" to linear representations of a different group G' on ordinary Hilbert space. Here, G' is a particular central extension of G, and it turns out to be the universal covering group of G in many cases. This is why we care about representations of $SU(2)$ and $SU(2) \times SU(2)$ rather than just those of $SO(3)$ and $SO(3,1)$. It is where half-integer spins come from.

3.3 Information Content in an SES

As we will see shortly, there are "internal" and "external" ways of understanding the relationships between groups. In the internal view, an SES embodies the notion of normal subgroup and corresponding quotient group. In the external view, an SES embodies a way of combining two groups A and C into a third group B which setwise looks like $A \times C$ and incorporates their multiplications in some fashion.

The basic relationships are embodied in the following propositions. First, let's consider how we can build an SES from a normal/quotient relation between groups N and G, possibly along with attaching maps.

- **Prop 3.2:** Given group G and normal subgroup $N \lhd G$, there is an SES $e \to N \xrightarrow{i} G \xrightarrow{q} G/N \to e$.

  Pf: i is injective and q is surjective automatically. ker q is all group elements mapping to the $[e]$ class — which is (by definition) N. So Im i = ker q.
- **Prop 3.3:** Given a group G, a normal subgroup $N \lhd G$, and an attaching isomorphism $\alpha : G/N \to C$, we have an SES $e \to N \xrightarrow{i} G \xrightarrow{\alpha \circ q} C \to e$.

  Pf: i remains unchanged (and thus injective). Since α is an isomorphism, q being surjective implies $\alpha \circ q$ is as well. Also since α is an isomorphism, ker $(\alpha \circ q)$ = ker q = Im i.
- **Prop 3.4:** Given a group G, a normal subgroup $N \lhd G$, and an attaching isomorphism $\alpha : A \to N$, we have an SES $e \to A \xrightarrow{i \circ \alpha} G \xrightarrow{q} G/N \to e$.

  Pf: q remains unchanged (and thus surjective). Since α is an isomorphism, $i \circ \alpha$ remains injective and Im $(i \circ \alpha)$ = Im i = ker q.
- **Prop 3.5:** Given a group G, a normal subgroup $N \lhd G$, and two attaching isomorphisms $\alpha : A \to N$ and $\beta : G/N \to C$, we have an SES $e \to A \xrightarrow{i \circ \alpha} G \xrightarrow{\beta \circ q} C \to e$.

  Pf: All the arguments from the previous two propositions hold here as well.

It follows that *any* homomorphism between two groups gives rise to an SES.

- **Prop 3.6:** Given a surjective homomorphism $g : B \to C$, we have an SES $e \to \ker g \xrightarrow{i} B \xrightarrow{g} C \to e$.

  Pf: The First Isomorphism thm tells us $\ker g \triangleleft B$, so we have a canonical SES $e \to \ker g \xrightarrow{i} B \xrightarrow{q} B/\ker g \to e$. As described above, we can attach C if we have an isomorphism $\alpha : B/\ker g \to C$. The First Isomorphism thm also tells us that $\alpha([x]) = g(x)$ (for $x \in G$) is such an isomorphism and is well-defined (i.e., independent of the choice of x within an equivalence class). It is clear that $\alpha \circ q = g$, so the SES is that stated.

  - Sometimes an SES is written $e \to A \to B \xrightarrow{g} C \to e$. Typically, what is meant here (if we know that it is in fact intended as an SES) is that $A = \ker g$ and $f = i$ (inclusion). I.e. it is a form of the surjective homomorphism SES. Alternatively, it could mean that $A \approx \ker g$ and the attaching isomorphism f is implicit. It is best to avoid using such potentially-ambiguous expressions.

- **Prop 3.7:** Given *any* homomorphism $g : B \to C$, we have an SES. It is given by $e \to \ker g \xrightarrow{i} B \xrightarrow{g} f(C) \to e$.

  Pf: Relative to $g(C)$, g is surjective so we have the case in Prop 3.6.

I.e., given a normal/quotient relationship between G and N, we have a canonical SES as well as the ability to construct a variety of related SES's via attaching maps. Specifically, given *any* groups $A \approx N$ and $C \approx G/N$, along with *any* specific isomorphisms for those, we obtain derivative SES's as described.

Next, let's go in the opposite direction and consider what an SES says about the relationship between groups.

- **Prop 3.8:** Given an SES $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$, $f(A) \triangleleft B$ and $C \approx B/f(A)$.

  Pf: In an SES, g is a surjective homomorphism so the First Homomorphism thm tells us that $\ker g \triangleleft B$ and $C \approx B/\ker g$. However, $\ker g = \mathrm{Im}\, f$ in an SES, so $f(A) \triangleleft B$ and $C \approx B/f(A)$.

- **Prop 3.9:** Given an SES, $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$, we have the following related SES's:

  - (i) $e \to f(A) \xrightarrow{i} B \xrightarrow{q} B/f(A) \to e$ (where i and q are the inclusion and quotient maps)
  - (ii) $e \to A \xrightarrow{f} B \xrightarrow{q} B/f(A) \to e$
  - (iii) $e \to f(A) \xrightarrow{i} B \xrightarrow{g} C \to e$.
  - Pf: (i) $f(A) \triangleleft B$, so we have a canonical SES for it. (ii) f is an attaching isomorphism from A to $f(A)$, so we get the 2nd SES. (iii) g is a surjective homomorphism with $\ker g = \mathrm{Im}\, f$ so we get the 3rd SES.
  - We'll refer to these collectively as the **derived SES's** of $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$ and to (i) as the **core normal/quotient SES**.

From these, it is evident that a general SES is tantamount to its core normal/quotient relationship plus two attaching isomorphisms.

The next obvious question to ask is which SES's are materially distinct, where "materially" remains to be defined. To do so, we must introduce notions of equivalent and isomorphic SES's.

3.4 SES Morphisms, Equivalence, and Isomorphism

The first thing we must develop is a notion of a structure-preserving map between two SES's. I.e., a morphism.

- **Morphism between SES's**: Given SES $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$ and SES $e \to A' \xrightarrow{f'} B' \xrightarrow{g'} C' \to e$, a morphism h between them consists of three group homomorphisms $h_a : A \to A'$, $h_b : B \to B'$, and $h_c : C \to C'$ s.t. $h_b \circ f = f' \circ h_a$ and $h_c \circ g = g' \circ h_b$.
  - I.e., the following diagram must commute:

$$\begin{tikzcd}
e \arrow[r] & A \arrow[r, "f"] \arrow[d, "h_a"] & B \arrow[r, "g"] \arrow[d, "h_b"] & C \arrow[r] \arrow[d, "h_c"] & e \\
e \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r] & e
\end{tikzcd}$$

  - We'll collectively refer to the morphism maps (h_a, h_b, h_c) as h.

When it comes to groups, we typically only care about isomorphism classes. If two groups are isomorphic they are viewed as "the same" for most purposes. With SES's things are a bit more complicated. They are compound structures with several moving parts. It turns out there are three key distinct notions of SES's looking the same. These are plain old equality (i.e. $A = A'$, $B = B'$, $C = C'$, $f = f'$, and $g = g'$), SES-isomorphism, and SES-equivalence.

SES-isomorphism and SES-equivalence embody what we mean by SES's being "materially" identical. Which of them we care about depends on the specific application, much as whether we care about true equality or isomorphism of groups does. Let's begin with the weaker of the two: the notion of isomorphism.

- **Isomorphic SES's**: There exist SES-morphisms h, h' which are inverses.
  - This trivially is equivalent to the requirement that there exists an SES-morphism h s.t. h_a, h_b, and h_c are group isomorphisms.
  - Note that it is *not* sufficient that $A \approx A'$ and $B \approx B'$ and $C \approx C'$ alone. There must exist specific isomorphisms that also make the diagram commute:

$$\begin{tikzcd}
e \arrow[r] & A \arrow[r, "f"] \arrow[d, "h_a"] & B \arrow[r, "g"] \arrow[d, "h_b"] & C \arrow[r] \arrow[d, "h_c"] & e \\
e \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r] & e
\end{tikzcd}$$

  - Note that given isomorphisms h_a, h_b, and h_c which *do* satisfy the commutativity in one direction, their inverses automatically will in the other. So if we have a morphism of SES's and the component homomorphisms are isomorphisms, we have an isomorphism of SES's.
  - An SES-isomorphism basically says that if we can build B from A and C a certain way then we can build B' from A' and C' in an analogous way using the h maps.
  - We're now in a position to understand the term "series-equivalent" mentioned earlier.
    - Recall that two isomorphic normal subgroups of G are considered "series-equivalent" if the corresponding quotient groups are isomorphic as well. Series-equivalent basically says that $B' = B$, $A' \approx A$ and $C' \approx C$. Note that series-equivalence does *not* guarantee SES-isomorphism. We still need specific isomorphisms h_a, h_b, and h_c which make the diagram commute. We mentioned that isomorphism of normal subgroups implies isomorphism of the corresponding quotient groups when the normal isomorphism extends to an automorphism on B (or G in our earlier notation). However, we also mentioned that this is a sufficient but not necessary condition. It is precisely the cases for which the quotient *is* isomorphic but there is no automorphism of G which restricts to an isomorphism $N \to N'$ where SES-isomorphism fails. I.e., "series-equivalent non-automorphic" is tantamount to SES-non-isomorphic (when $N \approx N'$ and $G/N \approx G/N'$).
    - Note that even though $B = B'$, we need not assume $h_b = Id_B$. It can be any element of $Aut(B)$.
    - **Prop 3.10:** Given group G and two series-equivalent normal subgroups (i.e. $N \approx N'$ and $G/N \approx G/N'$), the corresponding SES's are SES-isomorphic iff there exists an isomorphism $N \to N'$ which extends to an automorphism

on all of G.

Pf: Suppose that N and N' are series-equivalent, and let's consider the implications for their canonical normal/quotient SES's $e \rightarrow N \xrightarrow{i} G \xrightarrow{q} G/N \rightarrow e$ and $e \rightarrow N' \xrightarrow{i'} G \xrightarrow{q'} G/N' \rightarrow e$. We have $N \approx N'$ and $G/N \approx G/N'$. For the two SES's to be isomorphic, we need an h_n, h_g, and h_q s.t. (i) $h_g \circ i = i' \circ h_n$ and (ii) $h_q \circ q = q' \circ h_g$. The first condition can be rewritten $h_g|_N = h_n$ (i.e., given $x \in N$, we need $h_g(x) = h_n(x)$). I.e., h_g restricts to h_n on N. Put another way, we require the existence of an isomorphism $h_n : N \rightarrow N'$ which extends to an automorphism h_g on all of G. It turns out that (ii) always can be satisfied when this is the case. To avoid confusion, we'll denote the classes of G/N' as $[]'$ where needed. We can define $h_q([x]) \equiv q' \circ h_g(x)$. First, let's show this is well-defined. Pick $x' \in [x]$. It can be written $x' = xn$ for some $n \in N$. $h_q([x']) = h_q([x])$ since $[x'] = [x]$. On the right, $h_g(x') = h_g(xn) = h_g(x)h_g(n)$. But $h_g(n) = h_n(n) \in N'$ since $h_g|_N = h_n$. Therefore, $h_g(xn) = h_g(x)n'$ for some $n' \in N'$. This means $q'(h_g(x)n') = [h_g(x)]' = q'(h_g(x))$. So it is well-defined. Note that it would *not* be well-defined for a general h_g, because $h_g(n)$ may not map to an element of N' in that case. Only because h_g restricts to h_n on N does this work! h_q is a homomorphism because $h_q([e]) = q' \circ h_g(e) = q' \circ e = [e]'$ and $h_q([xy]) = q'(h_g(xy)) = q'(h_g(x)h_g(y)) = q'(h_g(x))q'(h_g(y)) = h_q([x])h_q([y])$. It is injective because ker h_q consists of all classes $[x]$ s.t. $q' \circ h_g(x) = [e]'$. I.e. $h_g(x) \in N'$. But this just means $x \in h_a^{-1}(N')$ (again because $h_g|_N = h_a$ and both are isomorphisms), so $x \in N$. I.e., ker $h_q = [e]$ and h_q is injective. Given $[y]' \in G/N'$, is there a $[x] \in G/N$ s.t. $h_q([x]) = [y]'$? We need $q' \circ h_g(x) = [y]'$, which means $h_g(x) = yn'$ for some $n' \in N'$. We may as well pick $n' = e$, so $h_g(x) = y$. But both $x, y \in G$ and h_g is an isomorphism, so we can invert it. I.e., pick $x = h_g^{-1}(y)$ (map inverse, not multiplicative inverse). h_q therefore is surjective as well. h_q is a bijective homomorphism and thus an isomorphism.

* I.e., if N and N' are series-equivalent then their canonical normal/quotient SES's are isomorphic iff there exists an isomorphism $N \rightarrow N'$ which extends to an automorphism on G.

Why iff when we said it was a sufficient but not necessary condition? We must be careful what we are talking about. Given $N \approx N'$, the existence of an h_n which extends to h_g is a sufficient condition for $G/N \approx G/N'$ (i.e. for series-equivalence). Given series-equivalence (i.e. $N \approx N'$ *and* $G/N \approx G/N'$), this same condition is both necessary and sufficient for SES-isomorphism. However, given $N \approx N'$ it is perfectly possible to have $G/N \approx G/N'$ (i.e. series-equivalence) without SES-isomorphism. This can happen iff there is no h_n which extends to an h_g. Otherwise, we would have SES-isomorphism as well. Of course, in most cases where there is no h_n which extends to an h_g we have neither SES-isomorphism nor series-equivalence. More formally, let X be the statement "$N \approx N'$", let Y be "series-equivalence" (i.e. $N \approx N'$ and $G/N \approx G/N'$), let Z be "isomorphism of the corresponding SES's", and let C be the condition that "there exists some isomorphism $N \rightarrow N'$ which extends to an automorphism on G". Then $X \cap C \Leftrightarrow Z$ and $Z \Rightarrow Y$ (and thus $X \cap C \Rightarrow Y$). Obviously, $Y \Rightarrow X$ too (by its definition). However, $Y \not\Rightarrow C$ and $Y \not\Rightarrow Z$.

* The notion of "series-equivalent" should not be confused with the similar-sounding "equivalent SES's" we define below.

The next stricter notion of "sameness" is SES-equivalence.

- **Equivalent SES's**: $A = A'$ and $C = C'$ and there exists an SES morphism h s.t. $h_a = Id_A$ and $h_c = Id_C$.
  - Note that equivalence is not a vacuous concept. It is perfectly possible to have non-equivalent SES's with $A = A'$ and $C = C'$ and $h_a = Id_A$ and $h_b = Id_B$. To be SES-equivalent, we need an h_b which embodies both the difference between f and f' and the difference between g and g'.
  - Diagramatically, we require the following to commute:

$$\begin{tikzcd} e \arrow[r] & A \arrow[r, "f"] \arrow[d, "Id_A"] & B \arrow[r, "g"] \arrow[d, "h_b"] & C \arrow[r] \arrow[d, "Id_C"] & e \\ e \arrow[r] & A \arrow[r, "f'"] & B' \arrow[r, "g'"] & C \arrow[r] & e \end{tikzcd}$$

  - Put simply, we're changing only f, g, B between the two SES's *and* we have a compatible isomorphism h_b.
  - The commutativity requirements can be written $f' = h_b \circ f$ and $g = g' \circ h_b$.
  - **Prop 3.11:** SES-equivalence implies SES-isomorphism.

    Pf: SES-equivalence is a particular SES-isomorphism.
  - Note that it is perfectly possible to have non-equivalent SES's with $B = B'$. To be SES-equivalent, h_b must be an automorphism that embodies both the difference between f and f' and the difference between g and g'. For example, if B has distinct isomorphic normal subgroups (i.e. $f(A)$ and $f'(A)$) but no automorphism on B restricts to an isomorphism between them, there could be SES's $e \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow e$ and $e \rightarrow A \xrightarrow{f'} B \xrightarrow{g'} C \rightarrow e$ which not only are non-equivalent but are non-isomorphic. In that case, they would be series-equivalent non-automorphic, as discussed earlier.

Let's consider the difference between SES-equivalence and SES-isomorphism a bit.

- We've seen that the property of SES-equivalence implies the property of SES-isomorphism. The former is defined only when $A = A'$, $C = C'$, so it is natural to ask whether under those circumstances the converse holds too. I.e., when $A = A'$ and $C = C'$ is SES-equivalence the same as SES-isomorphism? The answer is no. We can have an SES-isomorphism which is not an SES-equivalence.
  - This is not as vacuous a question as it may seem at first glance. SES-isomorphism as a property (as opposed to a specific choice of SES-isomorphism) requires the existence of group isomorphisms h_a, h_b, and h_c s.t. the diagram commutes, while SES-equivalence as a property requires the existence of an SES-isomorphism with $h_a = Id_A$ and $h_b = Id_B$. Obviously, a general SES-isomorphism is not an SES-equivalence, even if $A = A'$ and $B = B'$. However, it is quite possible that if any SES-isomorphism exists (i.e. the property of SES-isomorphism holds) we always can obtain an SES-equivalence through some sort of machination (i.e. the property of SES-equivalence holds). Obviously, this would involve some other h'_b, presumably derived from h_a, h_b, and h_c. It turns out this is not possible in general. See https://math.stackexchange.com/questions/351581/equivalences-and-isomorphisms-of-short-exact-sequences for a discussion of this.
  - However, this converse *does* hold under certain circumstances, as the following proposition makes clear.
  - **Prop 3.12:** Given an SES-isomorphism h, there is an SES-equivalence iff $\exists k \in Aut(B)$ that simultaneously extends h_a (i.e. $k|_{f(A)} = h_a$) and lifts h_c (i.e. $g \circ k = h_c$).

    Pf: This literally is just a restatement of the commutativity requirement.

There are some unintuitive aspects to SES-equivalence and SES-isomorphism, so let's consider a few questions (several of which differ subtly).

- Warning: some authors use the word "equivalence" to refer to SES-isomorphism rather than SES-equivalence. These authors tend to not bother with defining the notion of SES-equivalence at all. This is not entirely unreasonable since we almost always are interested in SES-isomorphism classes rather than SES-equivalence classes. However, the fact that different authors use different conventions can lead to confusion — so care must be taken when encountering this term.
- Consider a general SES $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$. Can $A' \approx A$ and $B' \approx B$ and $C' \approx C$ but there exist no isomorphic SES with A', B', and C'? No, we always can build one.
  - As before, this is not a vacuous question. We know that a given pair of SES's need not be SES-isomorphic even if $A \approx A'$ and $B \approx B'$ and $C \approx C'$. There may simply be no choice of h which makes the diagram commute. But now we are asking whether we can find *any* SES involving A', B', and C' (in that order) which works. I.e., we have the freedom to pick f' and g'.
  - Pf: Since we know the three pairs of groups are isomorphic, let's choose some set of isomorphisms h_a, h_b, and h_c. We define $f' \equiv h_b \circ f \circ h_a^{-1}$ and $g' \equiv h_c \circ g \circ h_b^{-1}$. This forces the diagram to commute. Moreover, f' is injective and g' is surjective. This is because the composition of injective (surjective) maps is injective (surjective), and any isomorphism is both injective and surjective. They also satisfy ker $g' =$ Im f'. To see this, note that ker $h_c = \{e\}$ and ker $h_c \circ g =$ ker g. So ker $g' = (h_b^{-1})^{-1}(\text{ker } g) = h_b(\text{ker } g)$. On the other end, Im $f' = h_b(f(h_a^{-1})(A'))$. We therefore need $h_b(\text{ker } g) = h_b(f(h_a^{-1}(A')))$. Since h_b is an isomorphism, we can compose h_b^{-1} on the left to get ker $g = f(h_a^{-1}(A'))$. But $h_a^{-1}(A') = A$ since h_a^{-1} is surjective. So we need ker $g =$ Im f, which have from the first SES.
  - I.e., not only is there always an isomorphic SES, but for any given choice of specific isomorphisms h_a, h_b, and h_c we can find one.
  - Why not use this to solve the series-equivalent issue mentioned earlier? We have $N \approx N'$ and $G/N \approx G/N'$, so can't we just find an SES which is isomorphic — thus violating our earlier statement that this may not be possible? We have to be careful what precisely we are asking. In that case, we were dealing with normal/quotient SES's which have specific inclusion and quotient homomorphisms as part of their structure. We therefore did not have the freedom to pick f' and g'. If we ask whether there is *some* SES with $N' \approx N$ and $G/N' \approx G/N$ (and the same G) that is isomorphic, then the answer is yes. However it won't have i' and q' as its homomorphisms. In the series-equivalent non-automorphic case, it is impossible to find an h_n, h_g, and h_q which would lead to $f' = i'$ and $g' = q'$ via the method just described.
  - In a similar vein, why doesn't this give us an avenue to show the converse involving SES-equivalence? Suppose $A' = A$ and $C' = C$ and we have an SES-isomorphism. Can't we just pick $h_a = Id_A$ and $h_c = Id_C$ and then find an f' and g' which give us an SES-equivalence? Sure. In fact, we don't even need to start with an SES-isomorphism. Given any SES and any $B' \approx B$ and h_b, we can find an SES-equivalent SES. We never claimed we couldn't. After all, we're allowing ourselves freedom to pick any SES. It's only when we're confined to considering two specific SES's that it may be impossible to find a specific h_b.
- Now consider a normal/quotient SES $e \to N \xrightarrow{i} G \xrightarrow{q} G/N \to e$. Can $G \approx G'$ and $N \approx N'$ and $G/N \approx G'/N'$ but there exist no isomorphic normal/quotient SES with N' and G'? Surprisingly, the answer is yes.

  - The key difference from the previous case is that we have no attaching homomorphisms. I.e., we have no freedom to pick f' and g' because they are the inclusion and quotient maps. All we can pick are h_n, h_g, and h_q (i.e. h_a, h_b, and h_c adapted to our current notation). The essential problem is analogous to the one discussed earlier for series-equivalent normal subgroups (though in that case, $G = G'$). The first commutativity requirement is $i' \circ h_n = h_g \circ i$. I.e., $h_n = h_g|_N$. This can be satisfied iff $\exists$ an isomorphism h_g which restricts to an isomorphism between $N \triangleleft G$ and $N' \triangleleft G'$. Any h_g induces an isomorphism between N and *some* normal subgroup of G'. However, for a particular choice of N' there may be no h_g which takes N to it. The second commutativity requirement is $h_q \circ q = q' \circ h_g$. For a given h_g and h_q, there is no guarantee that h_g "lifts" classes of G to classes of G'. I.e., that it is compatible with q'. If it does, then h_q is the lift. Since we have locked down G'/N', we need the existence of an h_g which lifts classes.
  - How do we reconcile this with our previous result, given our claim that f and g are just attaching maps? Well, we never said they were *just* attaching maps. They're attaching maps plus some. Specifically, f incorporates the choice of normal subgroup $N = f(A)$. The freedom to choose f' and g' allows us to pick $N' = f'(A')$ as well. The equivalent question in our current internal language would be whether we always can find some suitable N' and h_n, h_g, and h_q. That extra flexibility *does* admit a solution.

- What if we also require $G = G'$ (instead of just $G \approx G'$)? Can $N' \approx N$ and $G' = G$ and $G/N' \approx G/N$ but there exist no SES-isomorphic SES with N'? The answer still is yes.
  - Note that $G = G'$ does *not* imply $h_g = Id_G$. We are free to pick *any* element of $Aut(G)$ which works.
  - The condition now is that $h_n = h_g|_N$ and h_g takes classes of G/N to classes of G/N'. There may or may not exist such an automorphism h_g.
  - We're now dealing with precisely the series-equivalent case from earlier. As mentioned, there are situations in which $N \approx N'$ and $G/N \approx G/N'$ but no there is no automorphism on G which restricts an an isomorphism between N and N'. I.e., there is no compatible h_n and h_g.
  - Even if N and G/N (and thus N' and G/N') are abelian, there still exist such cases.
  - See `https://groupprops.subwiki.org/wiki/Series-equivalent_not_implies_automorphic` for a table of such situations.

- Let's look at a more extreme example. Consider two SES's with the same A, B, and C. I.e., they have the same groups, not just isomorphic groups. All that differs between them is f and g. Does this guarantee that the SES's are SES-equivalent? No. In fact, they needn't even be SES-isomorphic. If just $f = f'$ or $g = g'$, we have an SES-isomorphism, but not necessarily an SES-equivalence.

  The case with both $f \neq f'$ and $g \neq g'$ is just what we discussed earlier. If $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$ and $e \to A \xrightarrow{f'} B \xrightarrow{g'} C \to e$ are SES-isomorphic there exists isomorphisms h_a, h_b, and h_c which make the diagram commute. In our case, these are automorphisms of A, B, and C. For the same reason compatible isomorphisms h_a, h_b, and h_c may not exist in the $A \approx A'$, $B \approx B'$, $C \approx C'$ case discussed above, compatible automorphisms may not exist when $A = A'$, $B = B'$, and $C = C'$. Perhaps an easier way to see this is is via the core normal/quotient relations. Two SES's with the same A, B, and C may have distinct normal-quotient relations. If $f(A) \neq f'(A)$, then there are different normal copies of A inside B, and distinct corresponding normal/quotient relations. What if $f = f'$? We have the same quotient group (which depends only on $f(A)$), but two distinct canonical isomorphisms α and α' from $B/f(A)$ to C (induced from g and g' by the First Isomorphism thm). Any two isomorphisms between $B/f(A)$ and C are related by an automorphism of $B/f(A)$ (or, equivalently, an automorphism of C). We therefore do have an automorphism of C which takes g to g'. Using $h_a = Id_A$ and $h_b = Id_B$ and this automorphism $\alpha \circ \alpha'^{-1}$ as h_c, we have an SES-isomorphism. However, since $h_c \neq Id_C$ (unless the two SES's are equal), there is no SES-equivalence. If instead, $g = g'$, then $\ker g = \ker g'$. Since $\ker g = f(A)$ and $\ker g' = f'(A)$ by the SES exactness relations, $f(A) = f'(A)$ and we have the same quotient group. But f and f' both are isomorphisms to $f(A)$, so by the same reasoning as before, $f \circ f'^{-1}$ is an automorphism of $f(A)$. We therefore have an SES-isomorphism given by $h_a = f \circ f'^{-1}$, $h_b = Id_B$, and $h_c = Id_C$.

- Now consider a different question. Suppose we have a normal/quotient SES $e \to N \xrightarrow{i} G \xrightarrow{q} G/N \to e$ and a specific automorphism $h_n : N \to N$. Is there an SES-automorphism (i.e. an SES-isomorphism from the SES to itself) involving h_n? The answer is no.
  - Obviously, any SES is SES-equivalent to itself. We're asking a different question: whether we can pick a suitable h_g and h_q s.t. $i \circ h_n = h_g \circ i$ (i.e. $h_g|_N = h_n$) and $q \circ h_g = h_q \circ q$ (i.e. $h_q([x]) = [h_g(x)]$, where we don't need $[]'$ notation since the equivalence classes are the same since N is the same in both cases). We still have the usual automorphism-restriction problem. Unless there exists an automorphism on G which restricts to the automorphism h_n on N, we don't have an SES-automorphism. The same issue arises if we fix h_q or h_g and ask whether we can pick the other two isomorphisms to create an SES-automorphism.

- Can two SES's have the same A and C but distinct (i.e. non-isomorphic) B's? They sure can.

  As a simple example, $B = A \oplus C$ always exists and is unique. If there is any non-trivial extension B' of A by C then it can't be isomorphic to B.

- Suppose $A \not\approx A'$ or $C \not\approx C'$. Obviously, any SES's involving these would be non-isomorphic, but is it possible that we'll get the same B despite this? I.e., can we build the same B from different pairs of groups? The answer is yes.
  - As a purely semantic point, whether we require $B = B'$ or accept $B \approx B'$ depends on whether we take the internal or external view. If we're building B from distinct building blocks then obviously we can't formally have $B = B'$ since there is no canonical identification of points in $A \times C$ with those in $A' \times C'$. However, in the internal view we obviously can. And from the standpoint of SES's we obviously can. We haven't defined these terms yet, so this is something to keep in mind for when we do.
  - As an example consider $B \equiv B_1 \oplus B_2 \oplus B_3$, the direct sum of three distinct (non-isomorphic) groups. We can write $B = (B_1 \oplus B_2) \oplus B_3$ (i.e. $A = (B_1 \oplus B_2)$ and $C = B_3$) or $B = B_1 \oplus (B_2 \oplus B_3)$ (i.e. $A = B_1$ and $C = B_2 \oplus B_3$). These are non-isomorphic SES's which produce the same B. As an even simpler example, we can write $B = A \oplus C$ and $B = C \oplus A$ and these are non-isomorphic SES's (assuming $A \not\approx C$, of course).

Let's next consider the relationship between an SES and the derived SES's mentioned earlier. Is an SES isomorphic to its derived SES's? The answer is yes, as the following two results show.

- **Prop 3.13:** An SES $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$ is isomorphic to its derived SES's.
  - Pf: $(e \to f(A) \xrightarrow{i} B \xrightarrow{g} C \to e)$: Pick $h_a = f$, $h_b = Id_B$, and $h_c = Id_C$. Then $Id_B \circ f = i \circ f$ and $Id_C \circ g = g \circ Id_B$.
  - Pf: $(e \to A \xrightarrow{f} B \xrightarrow{q} B/f(A) \to e)$: Pick $h_a = Id_A$ and $h_b = B$. For h_c we use α^{-1}, where α is the canonical isomorphism $\alpha : B/f(A) \to C$ from the First Isomorphism thm (given by $\alpha([x]) \equiv g(x)$, and which is guaranteed to be well-defined). I.e., $\alpha \circ q = g$. $Id_B \circ f = f \circ Id_A$ and $\alpha^{-1} \circ g = q \circ Id_B$. To see the latter, note that $\alpha^{-1} \circ g = \alpha^{-1} \circ \alpha \circ q = q$.
  - Pf: $(e \to f(A) \xrightarrow{i} B \xrightarrow{q} B/f(A) \to e)$: We combine the two. $h_a = f$, $h_b = Id_B$, and $h_c = \alpha^{-1}$. Then $Id_B \circ f = i \circ f$ and $\alpha^{-1} \circ g = q \circ Id_B$ just as before.
- **Prop 3.14:** If two SES's $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$ and $e \to A' \xrightarrow{f'} B' \xrightarrow{g'} C' \to e$ be isomorphic, then their derived SES's all are isomorphic to one another as well.
  - Pf: SES-isomorphism is a transitive property. We know that each SES is isomorphic to all its derivative SES's and the two SES's are isomorphic, so every pair of SES's involved has to be isomorphic. I.e., they're all in the same isomorphism class.
  - In terminology we have yet to introduce, the internal and external views look the same.

    But once again note that $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$ allows us freedom to pick N via the choice of f. We are *not* saying the information content is identical!
  - Put another way, all SES's that have the same core normal/quotient relationship are isomorphic.

    However, the converse is not true. Every isomorphism class need not have a unique core normal/quotient SES. As we have seen, it is quite possible for two distinct normal/quotient SES's to be isomorphic. Put another way, the partition of SES's by core normal/quotient relationship is a refinement of the partition by isomorphism class.

Finally, let's consider SES-automorphisms.

- **SES-automorphism**: An SES-isomorphism from an SES to itself. I.e. A, B, C, f, and g all are the same.
  - An SES-automorphism requires automorphisms h_a, h_b, and h_c s.t. $f \circ h_a = h_b \circ f$ and $h_c \circ g = g \circ h_b$.
  - Not every set of automorphisms $h = (h_a, h_b, h_c)$ has these properties. Even for a given h_b there may be no h_a and h_c which work. Nor need there exist *any* $h_b \neq Id_B$ for which a suitable h_a and h_b exist. I.e., a given SES may have no SES-automorphisms (other than identity).

- We lose no generality studying SES-automorphisms of a core normal/quotient SES. In that case, we need the following diagram to commute (where our automorphism is $h = (h_n, h_g, h_q)$).

$$\begin{tikzcd}
e \arrow[r] & N \arrow[r, "i"] \arrow[d, "h_n"] & B \arrow[r, "q"] \arrow[d, "h_g"] & G/N \arrow[r] \arrow[d, "h_q"] & e \\
e \arrow[r] & N \arrow[r, "i"] & G \arrow[r, "q"] & G/N \arrow[r] & e
\end{tikzcd}$$

- I.e., we need $i \circ h_n = h_g \circ i$ and $h_q \circ q = q \circ h_g$. Since i just is subset inclusion here, the first constraint can be read $h_n(n) = h_g(n)$. For a given h_g, this means $h_n = h_g|_N$. The second constraint tells us that $h_q([x]) = [h_g(x)]$, which means h_g must be compatible with the quotient classes. I.e., it must move quotient classes into quotient classes (though it can rearrange elements within each quotient class as well). Moreover, it must do so in a manner compatible with the behavior of group G/N (since h_q is an isomorphism). h_q then is determined from h_g as well. However, not every automorphism h_g has these properties. Once again, we come back to the issue that an automorphism on G need restrict to an automorphism on N nor lift an automorphism on G/N.

- But wait, can't we just pick an h_n and h_q and pretend they are attaching isomorphisms where A happens to be N and C happens to be G/N? We saw that as long as $f(A)$ is unchanged the attaching isomorphisms won't affect the core normal/quotient relationship. Well, that's true. The new SES is $e \to N \xrightarrow{h_n} G \xrightarrow{h_q \circ q} G/N \to e$ in that case. This *is* SES-isomorphic to $e \to N \xrightarrow{i} G \xrightarrow{q} G/N \to e$, but in a trivial way. The SES-isomorphism is just (h_n^{-1}, Id_G, h_q), which trivially satisfies our isomorphism constraints since $h_n^{-1} \circ h_n = Id_B \circ i = Id_N$ and $h_q \circ q = h_q \circ q \circ Id_B$. This simply tells us that, sure, we can unwind our pointless attaching maps via an SES-isomorphism. We still haven't found an h_b which creates an SES-automorphism, however.

- If we have an SES-auto-equivalence (i.e. a specific SES-equivalence h_b from an SES to itself), this is an SES-automorphism, of course. However, not every SES-automorphism is an SES-auto-equivalence.

  An SES-auto-equivalence requires that $h_b|_N = Id_N$ and that h_b only moves elements within each quotient class but leaves the quotient classes alone.

4 Isomorphisms and Splitting

We defined right-splitting and left-splitting as properties of an SES. We also mentioned that there may be more than one way to right-split an SES, and these can be materially different (as we will see, they lead to distinct semidirect products). Let's now consider whether splitting is an isomorphism-class property.

- **Prop 4.1:** If $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$ right-splits, C is isomorphic to a subgroup of B.

  Pf: We have an injective f, surjective g, Im f = ker g, and (necessarily injective) $h : C \to B$ s.t. $g \circ h = Id_C$. Because g respects quotient-classes, h picks out a single element of each class. If it picked two from the same class, g would map them to the same element of C and we wouldn't get Id_C on the round-trip. Since h is an injective homomorphism $C \to B$, it is an isomorphism $C \to h(C)$. Therefore, $C \approx h(C) \subset B$.

- **Prop 4.2:** If $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$ left-splits, C is isomorphic to a normal subgroup of B.

  Pf: We have an injective f, surjective g, Im f = ker g, and (necessarily surjective) $h : B \to A$ s.t. $h \circ f = Id_A$. We already have the isomorphism $\alpha : B/f(A) \to C$ given by $\alpha([x]) \equiv g(x)$ (which is well-defined since g is class-respecting). In general, we can't invert g (it's many-to-one), and we can't lift $B/f(A)$ to a subgroup of B by picking an element of each class which respects the group structure. However, we now have h to work with too. h is a surjective homomorphism, and thus has its own normal/quotient relation. Specifically, ker $h \triangleleft B$ and $A \approx B/\text{ker } h$. However, ker h is precisely the choice we are looking for. It picks a unique representative of each $B/f(A)$ class *and* constitutes a subgroup of B. How do we know it picks a unique rep? [Note: from now on in the proof, when we speak of quotient we mean $B/f(A)$ (as opposed to $B/\text{ker } h$), q is the corresponding quotient homomorphism, and "classes" refer to the elements of $B/f(A)$ as indexed by C.] We want to show that $q|_{\text{ker } h}$ is bijective. Since $h \circ f = Id_A$, h must restrict to the isomorphism $f^{-1} : f(A) \to A$ on $f(A)$. However $f(A)$ is just the class $[e]$ in $B/f(A)$. Consider a class $[x] \neq [e]$. The elements of $[x]$ are given by $xf(A)$ for some $x \notin f(A)$ (obviously, there are many ways to choose this x). h is a homomorphism, so it must map $xf(a)$ to $h(x)h(f(a)) = h(x)a$. There is a unique $a = h(x)^{-1}$ for which $h(xf(a)) = e$. I.e., $xf(h(x)^{-1}) \in B$ is mapped by h to e. If we chose some other $x' \in [x]$ instead, we would get $x'f(h(x')^{-1})$. However, since they are in the same class, $x' = xf(a')$ for some $a' \in A$. We therefore have $xf(a')f(h(xf(a'))^{-1}) = xf(a')f(h(f(a')^{-1}x^{-1})) = xf(a')f(h(f(a')^{-1}))f(h(x^{-1}))$. But $h \circ f = Id_a$, so $h(f(a'^{-1})) = a'^{-1}$ and we have $xf(a')f(a'^{-1})f(h(x^{-1})) = xf(h(x^{-1}))$. I.e., we get the same element of B. There is a unique element of each class which maps to e under h. We can use this to define a homomorphism $\beta : B/f(A) \to B$ given by $\beta([x]) = xf(h(x^{-1}))$, which as we just saw is the same for every x in the class. We thus have shown that C is isomorphic to a subgroup of B. That subgroup is ker h, which is normal in B.

- **Prop 4.3:** Left-splitting implies right-splitting.

  Pf: In the proof of Prop 4.2 we exhibited a homomorphism $\beta : B/f(A) \to B$ given by $\beta([x]) = xf(h(x^{-1}))$ (and which we saw is well-defined on classes), where $h : B \to A$ is our left-split homomorphism. We define a right-split homomorphism $h' : C \to B$ via $h' \equiv \beta \circ \alpha^{-1}$ (where $\alpha([x]) \equiv g(x)$ as usual). By construction, this satisfies $g \circ h' = Id_C$. It also is easy to see that $h'(C) = \ker h$.

- **Prop 4.4:** Given a right-splitting SES $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$ and right-split map k (with $K \equiv \text{Im } k \subset B$), we have (i) $K \approx B/f(A)$, (ii) $K \cap f(A) = \{e\}$, and (iii) $q|_K = k^{-1}$ is an isomorphism $K \to G/N$.

  Pf: We lose no generality working with a core normal/quotient SES. Since k is an injective homomorphism $G/N \to G$, it is an isomorphism $G/N \to K$. This proves (i). Since we have an SES, $\ker q = N$. Suppose there exists $x \in N \cap K$ with $x \neq e$. Since $x \in N$, $q(x) = [e]$. Since $x \in \text{Im } k$, we know $x = k([y])$ for some $[y]$. Moreover, $[y] \neq [e]$ because $k([e]) = e$. For a right-split map, $q \circ k = Id_{G/N}$. So we need $q(k([y])) = [y]$. But $q(k([y])) = q(x) = [e]$. So we need $x = e$, which violates our assumption. This proves (ii). To see (iii), consider $q \circ k = Id_{G/N}$. I.e. $q|_K \circ k = Id_{G/N}$. There can be only one inverse map to the isomorphism $k : G/N \to K$, so this must be $q|_K$.

  As a result, Prop 2.4 applies, and all the results of Prop 2.3 hold.

- **Prop 4.5:** Given any right-splitting SES $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$, there can be only one right-split map to a given suitable subgroup $K \subset B$. This is $k \equiv (g|_K)^{-1}$.

  – "Suitable" here means $K \approx B/f(A)$ and $f(A) \cap K = \{e\}$. It is necessary, but not sufficient.

  – I.e., if $\text{Im } k = \text{Im } k'$ then $k = k'$. We cannot have two distinct ways to right-split an SES to the same K.

  – Pf: This follows from Prop 4.4, but we'll show it directly. $g \circ k = g|_{\text{Im } k} \circ k = Id_C$. But $g|_{\text{Im } k'} \circ k' = Id_C$ too. $g|_{\text{Im } k}$ is an isomorphism $\text{Im } k \to C$ and $g|_{\text{Im } k'}$ is an isomorphism $\text{Im } k' \to C$. If $\text{Im } k = \text{Im } k'$ then k and k' both would be inverses of the same $g|_K$, so $k = k'$. Obviously, if $\text{Im } k \neq \text{Im } k'$ then they can differ. However, they still must be the same on the overlap region $\text{Im } k \cap \text{Im } k'$.

  – Note that we are *not* saying that the SES right-splits to *every* subgroup K s.t. $K \approx B/f(A)$ and $f(A) \cap K = \{e\}$. As we discussed in Prop 2.4, if $B/f(A)$ is infinite it is quite possible to have $K \approx B/f(A)$ yet for $q|_K$ to be isomorphic to a proper subgroup of $B/f(A)$ rather than all of $B/f(A)$. In that case, there would be no right-split map to K because $(q|_K)^{-1}(K) \subset K$. I.e. $(q \circ (q|_K)^{-1}) \neq Id_K$. Although no two elements of K sit in the same coset, it is possible that there are cosets with no elements of K.

  – We'll refer to the subgroups of B to which a given SES right-splits as that SES's "right-split-groups". Each is disjoint from $f(A)$ and has q_K as an isomorphism $K \to B/f(A)$.

- Given an SES and two right-split-groups K and K', there may or may not exist an SES-automorphism h that takes K to K' (i.e. with $h_b(K) = K'$). Since SES-automorphisms compose, we have transitivity and thus an equivalence relation. I.e., this defines a partition of the right-split-groups of a given SES. We'll term the classes of that partition "RSG-classes". I.e., right-split-groups K and K' are in the same RSG-class of an SES iff an SES-automorphism moves us between them.

- **Prop 4.6:** Right-splitting is an SES-isomorphism-class property in the following sense: (i) The property of right-splitting holds either for all members of an isomorphism class or for none, (ii) under a given isomorphism, every right-split-group of one SES is invertibly mapped to a corresponding right-split-group of the other SES, (iii) under a given isomorphism, RSG-classes are invertibly mapped to RSG-classes, (iv) all isomorphisms between two isomorphic SES's map RSG-classes in the same (invertible) way, and therefore (v) we meaningfully may speak of the RSG-classes of an isomorphism class of SES's.

- Pf: Suppose we have an SES-isomorphism h between $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$ and $e \to A' \xrightarrow{f'} B' \xrightarrow{g'} C' \to e$ and a choice of right-split-subgroup $K \subset B$. First, note that these are indeed SES's. $(q_K)^{-1} \circ q$ is a homomorphism $G \to K$ which (as mentioned) takes each g to the unique element of K in its coset. It is surjective because $(q_K)^{-1} \circ q|_K = Id_K$. Because $(q_K)^{-1}$ is injective, ker $((q_K)^{-1} \circ q) =$ ker $q = N$, and we have an SES. The same argument holds for the other SES. Now to the proof. (i,ii) Since h_b is an isomorphism, $h_b(K)$ is a subgroup of B'. Moreover, an isomorphism is bijective, so $h_b(N \cap K) = h_b(N) \cap h_b(K)$ and it follows that $h_b(N) \cap h_b(K) = \{e\}$. We know $g|_K$ is an isomorphism $K \to C$, so consider $g'|_{h_b(K)} = (g' \circ h_b)|_K$. For an SES-isomorphism, $g' \circ h_b = h_c \circ g$, so $g'|_{h_b(K)} = (h_c \circ g)|_K$. Since h_c is an isomorphism and $g|_K$ is an isomorphism, $g'|_{h_b(K)}$ is an isomorphism too. We've thus established that $h_b(K)$ is in the right-split-group of the second SES, with $(g'|_{h_b(K)})^{-1}$ as its right-split map. Performing the same procedure in the other direction returns us to K and $(g|_K)^{-1}$, so not only is right-splitting preserved but we have a bijection between the right-split-groups. (iii) suppose we have an SES-isomorphism h between two SES's and an SES-automorphism h' of the first which takes right-split-group K to K'. h induces an SES-automorphism of the 2nd SES via $h \circ h' \circ h^{-1}$, and this SES-automorphism takes $h_b(K)$ to $h_b(K')$. It is easy to see (by inverting this) that the isomorphism induces a bijection between the elements of the RSG-classes of the two SES's. (iv) Suppose we have two isomorphisms h and h' between the same two SES's. Then $h' \circ h^{-1}$ is an SES-automorphism of the 2nd SES which maps $h_b(K)$ to $h'_b(K)$, placing them in the same RSG-class. The same holds going the other way. (v) Given two SES's and an RSG-class of the first SES, all isomorphisms between them map it to the same RSG-class of the 2nd SES (and this is invertible if we go the other way). Because isomorphisms compose, this means that given an RSG-class of one SES, there is a unique corresponding RSG-class of every other SES in the isomorphism class. I.e., we have a natural bijection between the SES-classes of any two isomorphic SES's. [Any specific isomorphism then induces a bijection between the members of every pair of corresponding RSG-classes.] Since a choice of RSG-class for any SES fixes one for every other in this fashion, it makes sense to speak of the RSG-classes of the isomorphism-class. These may be labeled via the RSG-classes of any SES in that isomorphism class.

- Note that if we have a right-splitting SES, it is not possible to form an isomorphism to a non-right-splitting SES. Similarly, if we have two isomorphisms between two right-splitting SES's which take K to $h_b(K)$ and $h'_b(K)$ where $h_b(K) \neq h_b(K')$ then there is an SES-automorphism of the 2nd which takes $h_b(K)$ to $h'_b(K)$. I.e., of K' and K'' aren't in the same RSG-class of the 2nd SES, there can be no isomorphisms from the first taking K to them. We can have an isomorphism that takes K to K' or one which takes K to K'' or neither — but not both.

- Also note that there may be more than one right-splitting isomorphism class. All we've said is that we cannot mix right-splitting and non-right-splitting SES's in the same class.

- **Prop 4.7:** The property of left-splitting is preserved under SES-isomorphism.

  Pf: Let h be an SES-isomorphism between left-splitting SES $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$ and some other SES $e \to A' \xrightarrow{f'} B' \xrightarrow{g'} C' \to e$, and suppose $k : B \to A$ is a left-split map of the 1st (i.e. $k \circ f = Id_A$). Define $k' : B' \to A'$ via $k' \equiv h_a \circ k \circ h_b^{-1}$. Then $k' \circ f' = h_a \circ k \circ h_b^{-1} \circ f'$, but $h_b \circ f = f' \circ h_a$. Since h_a is an isomorphism, we can write $f' = h_b \circ f \circ h_a^{-1}$, and we have $k' \circ f' = h_a \circ k \circ h_b^{-1} \circ h_b \circ f \circ h_a^{-1} = h_a \circ k \circ f \circ h_a^{-1}$. But $k \circ f = Id_A$, so we get $h_a \circ h_a^{-1} = Id_{A'}$. Therefore, the 2nd SES left-splits as well.

- Since right-splitting and left-splitting are preserved across the entire isomorphism class, they also are preserved in each smaller core normal/quotient class. I.e., an SES left (right) splits iff all its derivative SES's left (right) split.

- We will see later that for any A and C there not only is a unique left-splitting SES-isomorphism class, but a unique left-splitting SES-equivalence class.

5 Some Notes about SES's

- An SES basically says we can build group B from groups A and C in a way which setwise is $A \times C$ (i.e. bijective with it) and where there is a core normal/quotient relation involved. This means we can define a group structure on $A \times C$ in a manner which is compatible with the multiplications on A and C. We will see how to do this explicitly later.
- Though setwise $B = A \times C$, topologically and algebraically it is not a direct product in general.

  This is analogous to the situation for a fiber bundle. In fact, there is a close relationship between SES's and fiber bundles. However, that is a topic for another time.
- It sometimes is said that the concept of a subgroup is dual to the concept of a quotient group. This is intuitive in the following sense. A subgroup can be thought of as an injective homomorphism. By the SES for normal/quotient groups, we can think of a quotient group as a surjective homomorphism. Since injections and surjections are categorically dual, it makes sense to think of quotient groups and subgroups as similarly dual. Whether the more useful duality is subgroup/quotient-group or normal-subgroup/quotient-group depends on the purpose.

  Bear in mind this is a duality, not a bijection. Isomorphic normal subgroups can induce non-isomorphic quotient groups.

A word of warning: there are some things which look like an SES but actually are not — even though they sometimes are called one. An SES *always* is a sequence of groups and homomorphisms. Here are two cases which sometimes can be confusing:

- The birthplace of exact sequences was algebraic topology. There, we encounter "short exact sequences" of chain complexes. These technically are not SES's in the sense we just described, though they are closely related.
  - Given a simplicial (or cellular) decomposition of a topological space X, we define C_n to be the free abelian group generated by the set of simplices (or cells) of dimension n for X. A chain complex is a sequence of homomorphisms $\cdots \leftarrow C_{n-2} \xleftarrow{\partial_{n-1}} C_{n-1} \xleftarrow{\partial_n} C_n \leftarrow \dots$ s.t. $\partial_{n-1} \circ \partial_n = 0$. These maps are collectively denoted ∂ (with the relevant ∂_n understood from the location in the chain complex), and we abbreviate the composition rule as $\partial^2 = 0$. A SES of chain complexes is a sequence of SES's, each between C_n's of a given dimension n. I.e., given three chain complexes, we line them up horizontally (one above the other) and then have an SES downward for each n. We also require that all the boxes commute. I.e., an SES of chain complexes is a sequence of individual SES's with the additional commutativity requirement vis-a-vis the ∂'s. The reason such things matter is that an SES of chain complexes gives rise to a long exact sequence (in the true sense) of homology groups for the three spaces whose chain complexes are involved. Dually, an SES of cochain complexes (whose homomorphisms are denoted d instead of ∂) gives rise to a long exact sequence of cohomology groups.
  - A canonical example, and one which can be particularly misleading, is the fiber bundle SES. This typically is written $e \to F \to E \to B \to e$ (or $F \to E \to B$ for short), where the fiber is F, the bundle is E, and the base space is B. None of these need be groups. Even for a principal bundle, B need not be a group — so it's not merely a matter of the type of fiber involved. What actually is being depicted is the SES of chain complexes for those three spaces. And indeed, this SES of chain complexes induces a long exact sequence relating the homology groups of those spaces. For a fiber bundle, there also is a long exact sequence of homotopy groups (in the order $F - E - B$ as well) which proves very useful when discussing Lie Groups (since their covering groups are fiber bundles) among other things.
- Another common SES-like sequence is $H \to G \to G/H$ for group G and general subgroup H. If H is normal, this is indeed an SES. However, sometimes people write this SES-like sequence more generally to describe the quotient *space*. In that case, we are not dealing with homomorphisms. I.e. q is just a map.

  In some cases, q may be a smooth fn rather than just a set map. Ex. for Lie Groups, G/H is a smooth manifold and q is a smooth fn.

6 External vs Internal View

We'll now describe three types of group operations or relationships between groups. In increasing order of generality and decreasing order of simplicity, these are the direct product, the semi-direct product, and the group extension. Each has a particular relationship to normality and SES's. We can view each in two ways three ways: as combining groups to form a new group, as describing a relationship between existing groups, or in terms of a SES.

Note that a lot of the elements of the proofs below may seem redundant. This is intentional. The goal is for each proof to roughly stand on its own (unless obviously derivative) to make clear where information is coming from and where it is going. This leads to similar arguments in different proofs.

- **External view**: A way of building a third group from two existing groups. This may be viewed as a binary operation.
- **Internal view**: A relationship between a group, a normal subgroup, and the corresponding quotient group.
- **SES view**: An SES with certain properties.

If we combine two groups A and C into a third group B via the external view, then the internal view describes the resulting relationship between A, B, and C. If we view A and C as related to an existing B, then the external view tells us how they can be combined into it from scratch. In both cases, we can construct a corresponding SES. Conversely, an SES with suitable properties tells us both how to construct B from A and C and how to view A

and C in the context of a normal/quotient relationship to B.

The three views are equivalent up to some syntactic sugar which may appear in one view but not another. They are completely equivalent modulo SES-isomorphism, as will be apparent when we discuss group extensions. Whether they are precisely equivalent beyond that depends on the details of how we define the SES-view. Some confusion studying the subject can arise from the different views used in different treatments, the cavalier way these often are handled, and whether the authors implicitly are working with SES-isomorphism classes or not.

6.1 Overview of External View Construction

Before delving into the specifics, let's preview what we'll be doing. This section may be more useful after reading the sections on direct products and semidirect products, as it references some elements we have yet to discuss.

In light of the machinery we've already developed, the internal view and SES view descriptions of all three operations will be relatively straightforward. The real challenge will be the external view. In this, we start with two unrelated groups (usually denoted A and C or H and K) and must construct a third group (usually denoted B or G) in a manner which produces a suitable normal/quotient relationship between the three groups. We'll do this by starting with a set $A \times C$ and then determining the constraints on any suitable multiplication on it. In doing so, it will be important not to confuse our set-labels with the group structure.

The basic problem is to construct a group by imposing a multiplication on the *set* $B = A \times C$ from those on A and C and any ancillary info (such as splitting-maps or a semidirect product homomorphism ϕ) such that:

- (i) A is isomorphic to a normal subgroup of B. I.e., there exists an injective homomorphism $f : A \to B$ s.t. $f(A) \triangleleft B$.
- (ii) C is isomorphic to the corresponding quotient group $B/f(A)$. I.e., there exists an isomorphism $\alpha : B/f(A) \to C$.
- (iii) enforces left-splitting if a direct product or right-splitting if a semidirect product, with splitting maps that are compatible with the provided information.

In all three operations we will consider (direct product, semidirect product, and general group extension), there are certain common aspects to the construction as well as some which differ. As mentioned, these concepts will be introduced later and elaborated on in great detail. This is a brief preview, and is not intended to make sense on a first reading.

- The following will remain the same:
  - (i) B looks set-wise like $A \times C$, in the sense that we usefully can label its points (a, c).

    "Usefully" means exactly that. We are not claiming this is a parametrization or reflects the group structure, just that it will be a convenient labeling scheme for the elements of B. See our comments about topology and parametrization below.
  - (ii) i takes a to (a, e). I.e., (A, e) constitutes the relevant normal subgroup.
  - (iii) We define a surjective homomorphism $g : B \to C$ which takes (a, c) to c.

    This is $q \circ \alpha$, with q the quotient map. I.e., C labels the relevant quotient group $B/i(A)$ and g is compatible with the quotient. Put another way, the quotient classes are (a, C), as we'll now explicitly state.
  - (iv) The quotient classes (i.e. cosets) $B/i(A)$ are of the form (a, C) (though they aren't necessarily distinct for all a's).

    I.e., the quotient slices are the same, regardless of which op is involved. This is not surprising when we consider that a direct product is a type of semidirect product is a type of general extension.

- (v) There is an induced isomorphism $\alpha([(a,c)]) = c$ between $B/i(A)$ and C.
- (vi) (e,e) always is the multiplicative identity on B.
- (vii) $(a,c) \cdot (a',c') = (m(a,a',c,c'), cc')$ for some function m we will construct. I.e., the 2nd half always multiplies as cc'.

  Intuitively, we move around the quotient group via cc' and then multiply within the slices. The latter can involve all sorts of twisting, embodied in the function m.

- (viii) $(a,c)^{-1} = (j(a), c^{-1})$ for some function j we will construct. I.e., the 2nd half always inverts as c^{-1}.

- What differs is:
  - (i) The specific multiplication on B. I.e., the function m.
  - (ii) The specific inverse on B. I.e., the function j.
  - (iii) Whether $B/i(A)$ (and thus C) is isomorphic to a subgroup of B and, if so, whether a normal subgroup.

    If we are confining ourselves to a direct product or semidirect products, these are additional constraints on the admissible multiplications on the set $B = A \times C$.

  - (iv) For a direct product, the left splitting map is $h(a,c) = a$.
  - (v) For a semidirect product, the right splitting map is $h'(c) = (e,c)$.

Once we've determined the constraints, we then can ascertain which multiplications on the *set* $B = A \times C$ are admissible. We also can add attaching maps afterward (keeping B unchanged), which apply automorphisms to A and C, thus producing any viable f and g we wish (we adjust any splitting-maps h and h' accordingly). The core $f(A) \triangleleft B$ and $C \approx B/f(A)$ relationships are unchanged by doing so, nor are whether the SES right or left splits (though the specific splitting maps and isomorphism map will be).

We'll conduct this entire procedure in gory detail in the addendum. For now, we'll build up by starting with the direct product, then moving to the semidirect product, and finally looking at general group extensions in all their hideous glory. But first, a brief word about labels and parametrization.

6.2 Quick Note on Topology

One important note about the constructions we will describe and the proofs we will employ: topology plays no role.

- In much of what we discuss, we'll be combining two existing groups A and C into some other group B. One of the premises is that B "looks like" $A \times C$ setwise. By this, we don't just mean B is bijective with $A \times C$, but also that we choose to label its points (a,c).
- This always can be done and should not be confused with a parametrization. We're simply naming points for convenience, so that when we talk about things like $a \cdot a'$ (using A''s multiplication) it will be clear what point we are referencing.
- Again, these are labels, *not* a global parametrization. Even if A and C are topological groups, we are not imposing the product topology or any other topology. We are not assuming that a global parametrization exists (i.e. a global homeomorphism to $A \times C$) or even that a local parametrization does. Even when B could admit a compatible topological structure (ex. as a fiber bundle) and/or smooth structure (i.e. as a manifold), we are not imposing one here.

- I.e. our construction of a multiplication on B is purely algebraic.
- Of course, its implementation for concrete groups may very well involve introducing specific parametrizations.

> This is akin to the difference between the group theory of a Lie Group and its manifold structure. We can speak of the group theory in terms of labels g and g' and $g \cdot g'$, without worrying about patches and parametrizations and the topology of G. However, to actually compute with a given group we must use concrete parametrizations — and all those considerations then become important.

- The gist is that our use of labels (a, c) for points in $A \times C$ is not problematic, even if the only compatible topological structures (i.e. those which make the group a topological group) are non-product topologies, and even if the only continuous parametrizations are local (i.e. it is a topological manifold).

> The same could be said of the mobius strip vs the unit square. Both are $I \times I$ setwise in the sense described. I.e. their points can be labeled (x, y) with $x, y \in [0, 1]$. Only when we impose a topology does the question arise whether a continuous global parametrization $S \to [0, 1]^2$ exists. In the case of the unit square, our labeling happens also to serve as a suitable parametrization (because I^2 is a closed subset of R^2, which has its own topology). For the mobius strip, there is no global parametrization. It is a manifold with boundary and requires at least two charts. In that case, our labeling is not a parametrization because there *is* no global homeomorphism with R^2. Nonetheless, we can identify specific points in each chart with our (x, y) labels. We just can't do so globally in a way which produces a homeomorphism (i.e. a continuous map with continuous inverse).

- On a related note, it is hard not to remark the conceptual similarity between semidirect products and fiber bundles. Both involve twisting via an automorphism of one object as we move around another object. As mentioned earlier, there is in fact a connection between the two, but that will be a topic for another time.

6.3 Direct Product

The direct product is the simplest way to combine two groups into a third which looks like their product set-wise.

- **External view**: Given two groups H and K, their direct product $H \oplus K$ is set-wise $H \times K$ with multiplication defined as $(h, k)(h', k') \equiv (hh', kk')$.

> It follows from the mult on H and K that (e, e) is the identity and $(h, k)^{-1} = (h^{-1}, k^{-1})$. It is easy to verify that this is in fact a group.

- **Internal view**: A group G with two normal subgroups N_1 and N_2 that are disjoint (in the sense that $N_1 \cap N_2 = \{e\}$) and s.t. every $g \in G$ has a decomposition $g = n_1 \cdot n_2$ for some $n_1 \in N_1$ and $n_2 \in N_2$. We write $G = N_1 \oplus N_2$.

> From Prop 2.3 and Prop 2.5, it follows that the decomposition $g = n_1 n_2$ is unique, $N_1 \approx G/N_2$, and $N_2 \approx G/N_1$.

- **SES view**: An SES $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$ which left-splits (and thus right splits, too). We write $B = A \oplus C$.

> Technically, it is an SES-isomorphism class. We will see that there is a unique such isomorphism class which left-splits for any choice of A and C. As we also will see, the SES-isomorphism class in question actually is an SES-equivalence class as well.

The direct product of two groups always exists and always is unique. Moreover, if $H \approx H'$ and $K \approx K'$ then $H \oplus K \approx H' \oplus K'$. Let's now prove some of these claims.

- **Prop 6.1:** The external view implies the internal view.

> Pf: Start with the external view. $(h, k)(h', e)(h, k)^{-1} = (hh'h^{-1}, e) \in (H, e)$, so $(H, e) \triangleleft H \oplus K$. Similarly, $(h, k)(e, k')(h, k)^{-1} = (e, kk'k^{-1}) \in (e, K)$, so $(e, K) \triangleleft H \oplus K$. The cosets in $(H \oplus K)/(H, e)$ are $(h, k')(H, e) = (something, k)$ and $q(h, k) = k$ under the quotient map. The map $\alpha : (H \oplus K)/(H, e) \to (e, K)$ given by $\alpha([(h, k)]) = (e, k)$ therefore is well-defined. It trivially is bijective and trivially is a homomorphism (and thus an isomorphism). So we have the internal view with $N_1 = (H, e)$ and $N_2 = (e, K)$.

- **Prop 6.2:** The internal view implies the external view.

> Pf: This follows directly from Prop 2.3 and Prop 2.5. We can label each g by its unique $n_1 n_2$ decomposition. I.e., we can label G as (set-wise) $N_1 \times N_2$. Since N_1 and N_2 commute with one another, the multiplication is $gg' = n_1 n_2 n'_1 n'_2 = n_1 n'_1 n_2 n'_2$. This is just the multiplication from the external view (we used (n_1, n_2) notation there instead).

- **Prop 6.3:** An external-view direct product $H \oplus K$ defines a left-splitting SES $e \to H \xrightarrow{i} H \oplus K \xrightarrow{q} K \to e$, where $i(h) \equiv (h, e)$ and $q(h, k) \equiv k$. The left split map is $h_1(h, k) = h$ and the corresponding right split map is $h_2(k) = (e, k)$.
  - Pf: All four maps trivially are homomorphisms given the external-view multiplication. i plainly is injective and q plainly is surjective. ker $q = (H, e)$ and Im $i = (H, e)$, so we have an SES. The left-split map trivially satisfies $h_1 \circ i = Id_H$ and the right-split map trivially satisfies $q \circ h_2 = Id_K$.
  - We can reverse everything to get another left-splitting SES $e \to K \xrightarrow{h_2} K \oplus H \xrightarrow{h_1} H \to e$ (which has q and i as its left and right split maps). We'll see shortly that $K \oplus H \approx H \oplus K$, though we don't have an SES-isomorphism (obviously, since $H \not\approx K$ in general).
  - Without changing the relevant core normal/quotient relation, we can expand this to a seemingly more general SES by replacing H and i with any A and f s.t. $f(A) = (H, e)$ and replacing K and q with any C and g s.t. $C \approx K$ and ker $g =$ ker q. However, as seen earlier all such SES's are isomorphic to our original one. In fact that original one is the derivative normal/quotient SES for them all.

- **Prop 6.4:** Given any left-splitting SES $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$ (with left-split map h_1 and corresponding right-split map h_2), we have the internal-view direct product $B = f(A) \oplus h_2(C)$.
  - Pf: Let $N_1 \equiv f(A)$, which is normal in B for an SES, and let $N_2 \equiv h_2(C)$. We saw in Props 4.2 and 4.3 that for a left-splitting SES, the right-split map h_2 is an isomorphism between C and a normal subgroup $h_2(C) \triangleleft B$. I.e., both N_1 and N_2 are normal in B. We also saw that $h_2(C) =$ ker h_1 for such an SES (and we know that $f(A) =$ ker g for any SES). So $N_1 \cap N_2 =$ (ker g) $\cap$ (Im h_2). However, $g \circ h_2 = Id_C$, so ker $(g \circ h_2) = \{e\}$. Since h_2 is injective, ker $h_2 = \{e\}$, and ker $(g \circ h_2) =$ ker $(g|_{\text{Im } h_2}) =$ (ker g) $\cap$ (Im h_2), so (ker g) $\cap$ (Im h_2) $= \{e\}$ (i.e. N_1 and N_2 are disjoint). What remains is to show that every element of $x \in G$ has a decomposition $n_1 n_2$. We'll show that $n_1 = (f \circ h_1)(x)$ and $n_2 = (h_2 \circ g)(x)$. Define $y \equiv f(h_1(x)) \cdot h_2(g(x))$. First consider $g(y) = g(f(h_1(x))) \cdot g(h_2(g(x)))$. Since $g \circ h_2 = Id_C$ and ker $g =$ Im f, this is just $e \cdot g(x) = g(x)$. I.e., y and x are in the same coset under $B/f(A)$. Now suppose they are different. Then $x = f(a)y$ for some $a \in A$. But $f(a)f(h_1(x)) \cdot h_2(g(x)) = f(ah_1(x)) \cdot h_2(g(x))$. We now know that x has the necessary decomposition (since $f(ah_1(x)) \in N_1$), but let's show $a = e$ (i.e. that our precise projection maps are correct). Consider $h_1(x) = h_1(f(a \cdot h_1(x))) \cdot h_1(h_2(g(x)))$. But we know that ker $h_1 =$ Im h_2, so $h_1(h_2(g(x))) = e$. We also know $h_1 \circ f = Id_A$ so $h_1(x) = ah_1(x)$ and $a = e$. We not only have shown that every x has a decomposition but we have exhibited it (and from Prop 2.3 we know it is unique).
  - As mentioned, this often is written $B = A \oplus C$, but that obscures the roles of the attaching and splitting maps.
  - Together with the previous result, this tells us that $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$ left-splits iff it is a direct product.

- **Prop 6.5:** : Any left-splitting SES $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$ is SES-equivalent to the direct-sum SES $e \to A \xrightarrow{i} A \oplus C \xrightarrow{\pi} C \to e$ (where $A \oplus C$ is the external-view direct sum and $i(a) = (a, e)$ and $\pi(a, c) = c$). Consequently, $B \approx A \oplus C$ in all such cases.
  - Pf: Let $k : C \to A$ be any left-split homomorphism. We know k is surjective. We need to exhibit an isomorphism $h_b : B \to A \oplus C$ for which $i = h_b \circ f$ and $g = \pi \circ h_b$. The obvious candidate is $h_b(b) = (k(b), g(b))$. Let's first verify that it satisfies the commutativity conditions. $(h_b \circ f)(a) = (k(f(a)), g(f(a)))$, but $k \circ f = Id_A$ and $g(f(a)) = e$ (since Im $f =$ ker g), so $(h_b \circ f)(a) = (a, e) = i(a)$. For the second condition, $(\pi \circ h_b)(b) = g(b)$ trivially, so $g = \pi \circ h_b$. Since $h_b(e) = (k(e), g(e)) = (e, e)$ and $h_b(bb') = (k(bb'), g(bb')) = (k(b)k(b'), g(b)g(b')) = (k(b), g(b))(k(b'), g(b'))$, where the latter is just the mult on $A \oplus C$, it is clear that h_b is a homomorphism. ker h_b is the set of all b s.t. $(k(b), g(b)) = (e, e)$. I.e., it is (ker k) $\cap$ (ker g). However, ker $g =$ Im $f = (A, e)$, and ker $k = k^{-1}(e)$. Since $k \circ f = Id_A$, ker $k|_{f(A)} = (e, e)$. So ker $k \cap$ ker $g = (e, e)$ and h_b is injective. Now consider some $(a, c) \in A \oplus C$. We need a b s.t. $h_b(b) = (a, c)$. I.e., we need $k(b) = a$ and $g(b) = c$. Since g is consistent with cosets and is surjective, $g^{-1}(c)$ is a coset. Pick any element $x \in g^{-1}(c)$, and let $a' \equiv k(x)$. Then pick $b = f(a \cdot a'^{-1})x$. This clearly has $g(b) = g(f(a \cdot a'^{-1}))g(x) = g(x)$ and $k(b) = k(f(a \cdot a'^{-1}))k(x) = a \cdot a'^{-1} \cdot a' = a$. Since h_b is a bijective homomorphism it is an isomorphism.
  - This tells us that the choice of left-split homomorphism is irrelevant. All that matters is whether the SES left-splits or not.
  - This also tells us that for the given A and C (in that order), there is a unique left-splitting SES-equivalence class.

- **Prop 6.6:** The direct product of H and K is unique.

  Pf: Clearly, the external-view construction is unique (we gave a specific set and group operation on it). In the internal-view, it's less obvious what we mean by uniqueness. In that case, we ask whether there can be a non-isomorphic group G' which has normal subgroups N_1' and N_2' isomorphic to N_1 and N_2 and satisfying the requirements of a direct sum. Since we know the SES-view is equivalent, it's easier to work with that (and ultimately, we'd be reduced to doing so anyway). In the SES-view, uniqueness follows directly from Prop 6.5.

- **Prop 6.7:** $H \oplus K \approx K \oplus H$.

  Pf: This is evident from the group-swap symmetry present in all three views. Let's verify it explicitly, however. In the external view, the map $\alpha : H \oplus K \to K \oplus H$ defined $\alpha(h,k) = (k,h)$ is an isomorphism. $\alpha(e,e) = (e,e)$, and $\alpha((h,k)(h',k')) = \alpha(hh',kk') = (kk',hh')$ while $\alpha(h,k)\alpha(h',k') = (k,h)(k',h') = (kk',hh')$ (the latter under the mult on $K \oplus H$), so the two are equal and α is a homomorphism. However, α trivially is bijective and a bijective homomorphism is an isomorphism.

  Note that there is no corresponding SES-isomorphism since $H \not\approx K$ in general.

- **Prop 6.8:** If $H' \approx H$ and $K' \approx K$ then $H' \oplus K' \approx H \oplus K$, and the corresponding SES's are SES-isomorphic too.

  - I.e., we can find isomorphisms s.t. the following diagram commutes:

$$\begin{tikzcd}
e \arrow[r] & H \arrow[r, "i"] \arrow[d, "\alpha"] & H \oplus K \arrow[r, "q"] \arrow[d, "\rho"] & K \arrow[r] \arrow[d, "\beta"] & e \\
e \arrow[r] & H' \arrow[r, "i'"] & H' \oplus K' \arrow[r, "q'"] & K' \arrow[r] & e
\end{tikzcd}$$

  - Pf: This is easiest seen in the external view, so let's do that first. Let $\alpha : H \to H'$ and $\beta : K \to K'$ be any isomorphisms. Consider the bijection $\rho : H \oplus K \to H' \oplus K'$ give by $\rho(h,k) \to (\alpha(h), \beta(k))$. This is a homomorphism because (i) $\rho(e,e) = (e,e)$ and (ii) $\rho((h,k)(h',k')) = \rho(hh',kk') = (\alpha(hh'), \beta(kk')) = (\alpha(h)\alpha(h'), \beta(k)\beta(k'))$ but also $\rho(h,k)\rho(h',k') = (\alpha(h),\beta(k))(\alpha(h'),\beta(k')) = (\alpha(h)\alpha(h'), \beta(k)\beta(k'))$.
  - Pf: Let's show that this in fact is an SES-isomorphism between $e \to H \xrightarrow{i} H \oplus K \xrightarrow{q} K \to e$ and $e \to H' \xrightarrow{i} H' \oplus K' \xrightarrow{q} K' \to e$. We must show that our α, β, and ρ make the SES-isomorphism diagram above commute. For this, we need $\rho \circ i = i' \circ \alpha$ and $\beta \circ q = q' \circ \rho$. Note that $\rho \circ i$ takes $h \to (h,e) \to (\alpha(h), e)$, while $i' \circ \alpha$ takes $h \to \alpha(h) \to (\alpha(h), e)$. Since q here is just $q(h,k) = k$, $\beta \circ q$ takes $(h,k) \to k \to \beta(k)$ while $q' \circ \rho$ takes $(h,k) \to (\alpha(h), \beta(k)) \to \beta(k)$. The diagram therefore commutes, and we have an SES-isomorphism.

- To summarize:

  - $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$ left-splits iff B is the direct product of A and C.
  - The direct product of two given groups is unique.
  - B can be a direct product of both A, C and non-isomorphic A', C' (ex. $A \oplus (B \oplus C) = (A \oplus B) \oplus C$).
  - $A \oplus C \approx C \oplus A$.

- Note that the "direct product" is a general construction in mathematics. With groups, people more often refer to the "direct sum". Formally, this is identical except when an infinite number of groups are involved. The direct product of an infinite number of groups consists of all indexed sets of elements (one from each) with arbitrary numbers of those elements allowed to be non-trivial, whereas the direct sum is the same but allows each indexed set (i.e. element of the direct sum) to have only a finite number of non-identity component elements.

6.4 Semidirect Product

The semidirect product may seem a bit arbitrary at first but, as we will see, it is nothing more than the middle child of a progression which begins with the direct product and ends with general group extensions. However, in some ways semidirect products are the most troublesome of the three. Direct products are simpler because they are unique up to isomorphism. Group extensions are technically more difficult to construct, yet conceptually easier because they are less constrained. Semidirect products are constrained in a particular way and have an extra moving part.

Let's start with a quick summary of the three views and then we'll discuss each in more detail, as well as the relationships between them.

- **External view** (aka Outer Semidirect Product): Given two groups H and K and a homomorphism $\phi : K \to Aut(H)$, we define a new group $G = H \rtimes_\phi K$, labeled setwise as $H \times K$ and with multiplication defined by $(h,k)(h',k') = (h\phi_k(h'), kk')$.

  - The multiplication on $Aut(H)$ is composition. So ϕ being a homomorphism means $\phi_{kk'} = \phi_k \circ \phi_{k'}$.

- **Prop 6.9:** It follows from the group axioms that (e,e) must be the identity and that the inverse must be $(h,k)^{-1} = (\phi_{k^{-1}}(h^{-1}), k^{-1})$. We then indeed have a group.

  Pf: (identity) $(e,e)(h,k) = (e\phi_e(h), ek) = (\phi_e(h), k) = (Id_H(h), k) = (h,k)$, so the only candidate for identity is (e,e). Similarly, $(h,k)(e,e) = (h\phi_k(e), ke) = (he, ke) = (h,k)$ because $\phi_k(e)$ is an automorphism applied to e and thus yields e. So (e,e) is the identity element.

  Pf: (inverse) $(h,k)(h,k)^{-1} = (h,k)(\phi_{k-1}(h^{-1}), k^{-1}) = (h\phi_k(\phi_{k-1}(h^{-1})), kk^{-1})$. However, ϕ is a homomorphism so $\phi_k \circ \phi_{k-1} = Id_K$, and this is just $(hh^{-1}, e) = (e,e)$. Therefore, the specified expression is the only candidate for the inverse. Similarly, $(h,k)^{-1}(h,k) = (e,e)$. To see this, we'll just show that $((h,k)^{-1})^{-1} = (h,k)$. The left side is $(\phi_k(\phi_{k-1}(h)), k)$. Since ϕ is a homomorphism, $\phi_k \circ \phi_{k-1} = \phi_e = Id_H$ as needed. So our expression for $(h,k)^{-1}$ behaves like a two-sided inverse.

  Pf: (associativity): Consider $((h,k)(h',k'))(h'',k'')$. This is $(h\phi_k(h'), kk')(h'',k'') = (h\phi_k(h')\phi_{kk'}(h''), kk'k'')$. Likewise, consider $(h,k)((h',k')(h'',k''))$. This is $(h,k)(h'\phi_{k'}(h''), k'k'') = (h\phi_k(h'\phi_{k'}(h'')), kk'k'')$. So we need $\phi_k(h')\phi_{kk'}(h'') \overset{?}{=} \phi_k(h'\phi_{k'}(h''))$. This follows because $\phi_{kk'}(h'') = \phi_k \circ \phi_{k'}(h'')$ and $\phi_k(h'\phi_{k'}(h'')) = \phi_k(h')(\phi_k \circ \phi_{k'})(h'')$. So our multiplication is associative.

- **Prop 6.10:** Given H and K and ϕ, and any isomorphism $\alpha : K' \to K$ and any isomorphism $\gamma : H \to H'$, we have (i) $H \rtimes_{\phi'} K' \approx H \rtimes_\phi K$ for $\phi' \equiv \phi \circ \alpha$ and (ii) $H' \rtimes_{\phi''} K \approx H \rtimes_\phi K$ for $\phi''_k \equiv \gamma \circ \phi_k \circ \gamma^{-1}$.

  * Pf: (i) Define an isomorphism $\beta : H \rtimes_{\phi'} K' \to H \rtimes_\phi K$ via $\beta(h,k) = (h, \alpha(k))$. This trivially is bijective and $\beta(e,e) = (e,e)$. For multiplication, $\beta((h,k)(h',k')) = \beta(h\phi'_k(h'), kk') = (h\phi'_k(h'), \alpha(kk'))$ and $\beta(h,k)\beta(h',k') = (h, \alpha(k))(h', \alpha(k')) = (h\phi_{\alpha(k)}(h'), \alpha(k)\alpha(k'))$. Since α is an isomorphism, the 2nd components match up. We thus need to show that $h\phi'_k(h') \overset{?}{=} h\phi_{\alpha(k)}(h')$. However, $\phi' = \phi \circ \alpha$, so $\phi'_k(h') = \phi_{\alpha(k)}(h')$ and we're done. (ii) Define an isomorphism $\delta : H \rtimes_\phi K \to H' \rtimes_{\phi''} K'$ via $\delta(h,k) = (\gamma(h), k)$. This trivially is bijective and $\delta(e,e) = (e,e)$. For multiplication, $\delta((h,k)(h',k')) = (\gamma(h\phi_k(h')), kk') = (\gamma(h)\gamma(\phi_k(h')), kk')$ and $\delta(h,k)\delta(h',k') = (\gamma(h),k)(\gamma(h'),k') = (\gamma(h)\phi''_k(\gamma(h')), kk')$. But $\phi''_k(\gamma(h')) = \gamma(\phi_k(\gamma^{-1}(\gamma(h')))) = \gamma(\phi_k(h'))$. So the two sides are equal and we're done.
  * Note that from the standpoint of the external-view, H and K are just groups. We don't care what we call them, and the notion of isomorphic groups is irrelevant. There's no master group in which they are embedded or that defines relationships. All the relationships will arise from the external-view construction itself. Put another way, our proposition really says that $H \rtimes_\phi K \approx H \rtimes_{\phi'} K \approx H \rtimes_{\phi''} K$ where $\alpha \in Aut(K)$ and $\gamma \in Aut(H)$. I.e., for given (isomorphism classes of) groups H and K, we have identified classes of ϕ's that result in isomorphic constructions $H \rtimes_\phi K$. I.e., for a given H and K, we have an equivalence relation on the ϕ's. However, this needn't be the same as the isomorphism classes of $H \rtimes_\phi K$. It is possible that there are other isomorphisms too. I.e., it is a refinement of the isomorphism classes of $H \rtimes_\phi K$.
  * Prop 6.10 tells us two things: (i) we don't really need to consider isomorphic H''s or K''s because any ϕ we build with them can be mapped to a ϕ built from H and K and (ii) even when we fix H and K, ϕ's related by members of $Aut(H)$ and/or $Aut(K)$ in certain ways lead to group-isomorphic constructions. (i) tells us we can fix an H and K and vary ϕ alone without loss of generality, which really just makes our bookkeeping a bit simpler. (ii) tells us that for a given H and K, we can partition the ϕ's into classes s.t. all the members of a given class lead to group-isomorphic constructions. We'll call these PA-classes (for ϕ-automorphism classes).

    Note that members of distinct PA-classes may lead to isomorphic constructions as well. I.e., the partition of the space of ϕ's into PA-classes is a refinement of the partition by group-isomorphic constructions.

- The subscript in $H \rtimes_\phi K$ often is omitted and people write $H \rtimes K$, with the choice of ϕ implicit. This makes sense for the internal view below (where N and K are specified subgroups of G), but less so for the external-view, where we need ϕ in order to understand the relationship of H and K to $H \rtimes_\phi K$. Some people also write $K \ltimes H$ (or $K \ltimes_\phi H$) instead.
- Note that ϕ is nothing other than an action of K on H. All we are saying is that we have two groups and an action of one on the other.

  This action need not be free or transitive. ϕ is a homomorphism and need not be injective or surjective. It is quite possible for $\phi_k(h) = h$ for some $h \neq e$ and $k \neq e$, and there is no requirement that for every h, h', $\exists k$ s.t. $\phi_k(h) = h'$.

- **Internal view** (aka Inner Semidirect Product): Given a group G, a normal subgroup $N \triangleleft G$, and a subgroup $K \subset G$ s.t. $N \cap K = \{e\}$ and $G = NK$, we call G the semidirect product $N \rtimes K$.

- Recall that $G = NK$ just means that every element of G can be written $g = nk$ for some $n \in N$ and $k \in K$.
- Note the similarity to the direct product definition. The only difference is that K is not normal here.
- Equivalent definition: A group G and $N \triangleleft G$ and $K \subset G$ s.t. $N \cap K = \{e\}$ and $q|_K : K \to G/N$ is an isomorphism.

  Pf: Prop 2.4 gives us this in one direction and Prop 2.3 gives us it in the other.
- Note the freedom we have here. We can pick K if more than one suitable option is available, but once we've done so, the semidirect product is locked down. Also note that *any* $K \subset G$ s.t. $N \cap K = \{e\}$ and $q|_K$ is an isomorphism gives rise to a semidirect product $N \rtimes K$. However, this does not mean all such products are distinct. It is quite possible that $N \rtimes K \approx N \rtimes K'$ for two such subgroups. We'll now see one important case of this.
- **Prop 6.11:** Given two internal-view semidirect products with the same G and N, but different K and K', if there exists an automorphism on G which restricts to an automorphism on N and maps K to K' then $N \rtimes K \approx N \rtimes K'$.

  Pf: There is nothing to prove. The automorphism on G is precisely the isomorphism $N \rtimes K \approx N \rtimes K'$. We need it to take K to K' and we need it to preserve N, both of which it does by assumption.

  This is a sufficient but not necessary condition. There can be "series-equivalent non-automorphic" cases as well (as discussed earlier).

- **SES-view**: A semi-direct product is a right-splitting isomorphism class of SES's along with an RSG-class.

  Recall that RSG-class and its meaning in the context of an isomorphism class are discussed under Prop 4.6.

  Note that (using core normal/quotient SES notation), an RSG-class consists precisely of a set of K's satisfying Prop 6.11 for the internal view. I.e., the right-split freedom we have in the SES-view is the same as that in the internal-view.

These three views are materially equivalent modulo isomorphism. Let's now see this formally.

- **Prop 6.12:** Given an internal-view semidirect product, we have a corresponding SES-view one.

  Pf: We can get the SES-view two ways, but they are related in a trivial way. (i) Because $N \triangleleft G$, we have an SES $e \to N \xrightarrow{i} G \xrightarrow{q} G/N \to e$. Using $q|_K$ formulation of the internal view, we have an isomorphism $q|_K : K \to G/N$. Because $K \subset G$, we can use $(q|_K)^{-1} : G/N \to K \subset G$ as our right-split map. It is a homomorphism and trivially has $q \circ (q|_K)^{-1} = Id_{G/N}$. So K is in fact a right-split-group of our SES. We then pick the RSG-class containing K. As we saw in Prop 4.6, the entire SES-isomorphism class is right-splitting. We then have a unique RSG-class for every other SES in that isomorphism class. As discussed, this is what is meant by the RSG-class of the isomorphism class. (ii) We also have the SES $e \to N \xrightarrow{i} G \xrightarrow{\pi_2} K \to e$. We saw in Prop 2.3 that π_2 is a surjective homomorphism and that $\ker \pi_2 = N$, so this is indeed an SES. The right-split map is just subset inclusion $i' : K \to G$. This is an injective homomorphism, and $\pi_2 \circ i' = \pi_2|_K = Id_K$ so i' is indeed a right-split map. We then pick the isomorphism class containing this SES and RSG-class containing K. Note that the two give the same SES-view. (i) is just the core normal/quotient SES of (ii), so the two SES's are isomorphic. Moreover, there is an isomorphism that maps $K \subset G$ in (i) to $K \subset G$ in (ii). It is given by $h_a = Id_N$, $h_b = Id_G$, and $h_c = (q|_K)^{-1}$. Therefore, K is in the RSG-class for both SES's. Put another way, K relative to SES (i) and K relative to SES (ii) are in a common RSG-class of the isomorphism-class.

- **Prop 6.13:** Given an SES-view semidirect product, we have a corresponding internal-view one.

  We actually have a class of internal-view ones, but they all are isomorphic to one another.

  Pf: Without loss of generality, consider a core normal/quotient SES $e \to N \xrightarrow{i} G \xrightarrow{q} G/N \to e$ and let K be a member of the RSG-class for the SES-view semidirect product. As we saw in Prop 4.4, $q|_K$ is an isomorphism $K \to G/N$ and $N \cap K = \{e\}$. This gives us an internal-view semidirect product. Moreover, given any other K' in the same RSG-class, we have an SES-automorphism which takes K to K'. However, an SES-automorphism is just an automorphism on G which satisfies the conditions of Prop 6.11. I.e., given a right-splitting SES-isomorphism class and a RSG class of it, all the internal-view semidirect products we derive from any SES in it and any right-split-group in that RSG class for that SES will be group-isomorphic to one another.

- **Prop 6.14:** Given an external-view semidirect product, we have a corresponding SES-view one.

  Pf: We are given groups H and K and a homomorphism $\phi : K \to Aut(H)$. The relevant SES is $e \to H \xrightarrow{i} H \rtimes_\phi K \xrightarrow{q} K \to e$, where $H \rtimes_\phi K$ is the external-view semidirect product, $i(h) = (h, e)$ and $q(h, k) = k$, and the right-split map is $j(k) = (e, k)$ [we denote it j here since h and k already are in use]. i trivially is injective and q trivially is surjective. Im $i = (H, e)$, and ker $q = (H, e)$. Since $i(e) = (e, e)$ and $i(hh') = (hh', e)$ and $i(h)i(h') = (h, e)(h'e) = (h\phi_e(h'), e) = (hh', e)$, i is a homomorphism. Since $q(e, e) = e$ and $q((h, k)(h', k')) = q(h\phi_k(h'), kk') = kk' = q(h, k)q(h', k')$, q also is a homomorphism. We thus have an SES. As for the right-split, j trivially satisfies $q \circ j = Id_K$. To show it is a homomorphism, we note that $j(e) = (e, e)$ and $j(kk') = (e, kk') = (e, k)(e, k') = j(k)j(k')$ since $(e, k)(e, k') = (e\phi_k(e), kk') = (e, kk')$. We then take the SES-isomorphism class of our SES and the RSG-class of (e, K) (for our SES).

  Even though ϕ doesn't explicitly appear in i or q, it implicitly appears in the multiplication on $H \rtimes_\phi K$, as is apparent in the proof.

Why doesn't this left-split too? To left-split, we would need a homomorphism $j' : H \rtimes K \to H$ which gives us $j' \circ i = Id_H$. Obviously, we can do this for (H, e), but extending it to all of $H \rtimes K$ in general is not possible. Ex. one simple candidate is $j'(h, k) = h$, but this won't work. Why? $j'((h, k)(h', k')) = j'(h\phi_k(h'), kk') = h\phi_k(h')$, which is not hh' as hoped. Another candidate is $j'(h, k) = \phi_{k^{-1}}(h)$. This gives us $(j' \circ i)(h) = \phi_e(h) = h$ so it satisfies the condition. In that case, $j'((h, k)(h', k')) = j'(h\phi_k(h'), kk') = \phi_{(kk')^{-1}}(h\phi_k(h')) = \phi_{(kk')^{-1}}(h) \cdot (\phi_{k'^{-1}} \circ \phi_{k^{-1}}(h\phi_k(h'))) = \phi_{(kk')^{-1}}(h)\phi_{k'^{-1}}(h')$. This is not $\phi_{k^{-1}}(h) \cdot \phi_{k'^{-1}}(h')$, so it fails too. Note that the reason we can right split isn't because the 2nd component multiplies to kk'. As we will see, the multiplication on a general group extension has this property too but it does *not* right-split. The ability to right-split is effected by the particular nature of our 1st-component multiplication rule. This is in fact the most general form for which the SES *does* right-split.

Our right-split map $j(k) = (e, k)$ in the external-view is independent of ϕ and seems pretty universal. Why can't we use it to right-split *any* SES? As mentioned earlier, we *always* can pick a section (i.e. an injective fn which picks an element of every class and for which $q \circ j = Id_K$). However, it may not be a homomorphism. Our current j is just such a section. In the case of the multiplication on $H \rtimes_\phi K$ we defined, the proof above shows that it is indeed a homomorphism. However, for a general SES this is not the case. As we will see, such an SES embodies a group extension, and the obstruction will be evident when we exhibit the multiplication on it.

There appears to be a mismatch in freedom of choice. In the SES-view, we have freedom to pick an RSG-class for the isomorphism class of the SES, but in the external-view we have freedom to choose any homomorphism ϕ. This seems like far broader latitude than just picking an RSG class. We will have more to say about this shortly.

- **Prop 6.15:** Given an internal-view semidirect product, we have a corresponding external-view one.

Pf: We are given G, $N \triangleleft G$, $K \subset G$ s.t. $N \cap K = \{e\}$ and $G = NK$. We define the external view as $H \equiv N$, $K(ext) \equiv K(int)$ (i.e. K is the same in both), and $\phi_k(n) \equiv knk^{-1}$. For a given $k \in K \subset G$, this is just the restriction of an inner-automorphism of G to N. However, an inner-automorphism of G restricts to an automorphism on N, so ϕ_k is indeed in $Aut(H = N)$. What remains is to show that ϕ is a homomorphism from K to $Aut(N)$ We need only show that $\phi_e = Id_N$ and $\phi(kk') = \phi_k \circ \phi_{k'}$ since composition is the multiplication in $Aut(N)$. For the identity, $\phi_e(n) = ene = n$, so $\phi_e = Id_N$. For multiplication, $\phi_{kk'}(n) = kk'nk'^{-1}k^{-1} = \phi_k(\phi_{k'}(n))$. Lastly, we must show that the resulting $H \rtimes_\phi K \approx G$. Define isomorphism $\gamma : N \rtimes_\phi K \approx G$ via $\gamma(n, k) \equiv n \cdot k$. Then $\gamma(n, k)\gamma(n', k') = nkn'k'$. On the other hand, $\gamma((n, k)(n', k')) = \gamma(n\phi_k(n'), kk') = n\phi_k(n')kk' = nkn'k^{-1}kk' = nkn'k'$. We therefore have a homomorphism. ker $\gamma = (e, e)$, so γ is injective. It is surjective because for an internal-view semi-direct product every $g = nk$ for some $n \in N$ and $k \in K$. So γ is a bijective homomorphism and therefore an isomorphism.

- **Prop 6.16:** Given an SES-view semidirect product, we have a corresponding external-view one.

Pf: Prop 6.13 takes us from $e \to N \xrightarrow{i} G \xrightarrow{q} G/N \to e$ with right-split map $j : G/N \to G$ to an internal-view semidirect product with G, N, and $K = \text{Im } j$. Prop 6.15 then takes us from this to the external-view semidirect product $N \rtimes_\phi (\text{Im } j)$, where $\phi_k(n) = knk^{-1}$ for $k \in \text{Im } j$ (i.e. we use the ambient G to define the relevant automorphisms).

- **Prop 6.17:** Given an external-view semidirect product, we have a corresponding internal-view one.

Pf: Prop 6.14 takes us from H, K, and ϕ to $e \to H \xrightarrow{i} H \rtimes_\phi K \xrightarrow{q} K \to e$ where $i(h) = (h, e)$ and $q(h, k) = k$, and the right-split map is $j(k) = (e, k)$. Prop 6.13 then takes us to $G = H \rtimes_\phi K$, $N = (H, e)$, and $K = (e, K)$.

- As mentioned, there may seem to be an information mismatch. The internal-view and SES-view agree that we have a distinct semidirect product for every RSG-class of a right-splitting isomorphism class of SES's (although these "distinct" semidirect products still could happen to be isomorphic). However, the external-view seems to have a lot more freedom via its ϕ.

  - Note that from the standpoint of the internal-view it makes sense to speak of distinct isomorphic subgroups K and K' of G, but (as we discussed earlier) from the external-view standpoint it does not. K is an isolated group. Anything isomorphic to it can be considered the same group. We saw in Prop 6.10 that given any H, K, and ϕ, if we have isomorphisms $\alpha : K' \to K$ and $\gamma : H \to H'$, there is a ϕ' for which $(H' \rtimes_{\phi'} K') \approx (H \rtimes_\phi K)$. So where does the ability to choose a subgroup of G come from? The construction $G \equiv H \rtimes_\phi K$ tells us *how* K embeds in G. I.e., ϕ itself identifies how K embeds as a subgroup of G. Or, more precisely, it identifies the relevant class of subgroups vis-a-vis Prop 6.11.

  - Let's fix H and K. Do the PA-classes defined in the discussion of Prop 6.10 correspond to the RSG-classes from the SES-view (and thus the automorphism-related classes of the internal-view)? The following propositions tell us they do.

  - **Prop 6.18:** Given groups H and K, and external-view homomorphisms ϕ and ϕ' which are related by $Aut(H)$ and/or $Aut(K)$ as described in Prop 6.10 (i.e. in the same PA-class) we know that $H \rtimes_\phi K \approx H \rtimes_{\phi'} K$. The corresponding SES-view (and thus internal-view) semidirect products are in the same RSG-class of the same isomorphism class.

Pf: Let's consider the two cases from Prop 6.10 separately. (i) Let $\phi' = \phi \circ \alpha$ for $\alpha \in Aut(K)$, and denote $G' \equiv H \rtimes_{\phi} K$ and $G' \equiv H \rtimes_{\phi'} K$ The relevant right-splitting SES's are $e \to H \xrightarrow{i(h)=(h,e)} G \xrightarrow{q(h,k)=k} K \to e$ with right-split map $j(k) = (e, k)$ and $e \to H \xrightarrow{i'(h)=(h,e)} G' \xrightarrow{q'(h,k)=k} K \to e$ with right-split map $j'(k) = (e, k)$. Although these look the same (they have the same H, K, labeling, form of i, form of q, and form of j), bear in mind that $H \rtimes_{\phi} K$ and $H \rtimes_{\phi'} K$ are distinct groups. The embedding of K could be different in each. I.e., (e, K) could look quite different in the two groups. Let's construct the relevant SES-isomorphism class and RSG-class. In Prop 6.10 we saw that $\beta(h, k) \equiv (h, \alpha(k))$ is a group-isomorphism between the two constructions that took Im j to Im j' (i.e. the copy of (e, K) in G to the copy of (e, K) in G'). [Note that technically we're using α in the opposite direction as the proposition here, but it doesn't matter since $K' = K$]. This is pretty much what we need. Define our SES-isomorphism as $h_h \equiv Id_H$, $h_g \equiv \beta$, and $h_k \equiv \alpha$. Then we need $h_g \circ i = i' \circ h_h$ and $q' \circ h_g = h_k \circ q$. Note that $\alpha(e) = e$, $h_g(i(h)) = (h, e)$, and $i'(h_h(h)) = i'(h) = (h, e)$, so the first is achieved. The second requires $q'(\beta(h, k)) = \alpha(q(h, k))$. But $q'(h, \alpha(k)) = \alpha(k)$, while $\alpha(q(h, k)) = \alpha(k)$. We thus have our SES-isomorphism. As for the RSG-class, $(e, K) \subset G$ is mapped by β to $(e, \alpha(K)) \subset G'$. But α is an automorphism, so as a group $(e, \alpha(K))$ is just (e, K) (though the elements in it are rearranged by the automorphism, of course). I.e., we have the same RSG-class. So we've established that a specific isomorphism class and RSG-class are involved. For (ii) we do much the same. Let $\phi'_k \equiv \gamma \circ \phi_k \circ \gamma^{-1}$ (with $\gamma \in Aut(H)$). In that case, the two SES's look the same as above (but with our new ϕ' of course), and Prop 6.10 provides us with an isomorphism $\delta(h, k) \equiv (\gamma(h), k)$ between G and G'. We define our SES-isomorphism to be $h_h \equiv \gamma$, $h_g \equiv \delta$, and $h_k \equiv Id_K$. The first condition is $h_g \circ i = i' \circ h_h$. The left side is $h_g(i(h)) = h_g(h, e) = (\gamma(h), e)$, while the right side is $i'(h_h(h)) = i'(\gamma(h)) = (\gamma(h), e)$, so the first condition is met. For the second condition, we need $q' \circ h_g = h_k \circ q$. This is met because $q'(h_g(h, k)) = q'(\gamma(h), k) = k$ and $h_k(q(h, k)) = h_k(k) = k$. Finally, we note that $(e, K) \subset G$ trivially is mapped by δ to $(e, K) \subset G'$. Once again, we've established that a specific isomorphism class and RSG-class are involved.

- **Prop 6.19:** Given two isomorphic SES's $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$ and $e \to A' \xrightarrow{f'} B' \xrightarrow{g'} C' \to e$ and a given RSG class for that isomorphism class, we saw that we have corresponding external views. These can be expressed in terms of a common H and K and two distinct ϕ's, and those ϕ's are in the same PA-class (i.e. related as in Prop 6.10).

Pf: Without loss of generality, we can consider core normal/quotient SES's, $e \to N \xrightarrow{i} G \xrightarrow{q} G/N \to e$ and $e \to N' \xrightarrow{i'} G' \xrightarrow{q'} G'/N' \to e$. The RSG class is a choice of suitable $X \subset G$ (with corresponding choice $X' \subset G'$ under any SES-isomorphism). [We call it X because we'll use K for a different purpose.] Suppose we pick a specific SES-isomorphism $h = (h_n, h_g, h_q)$ s.t. $i' \circ h_n = h_g \circ i$ and $q' \circ h_g = h_q \circ q$. Then $X' = h_g(X)$. The corresponding external-view to the first SES via Prop 6.16 is $H \equiv N$, $K \equiv X$, and $\phi_k(n) \equiv knk^{-1}$. Similarly, the second corresponding external-view is $H' \equiv N'$, $K' \equiv X' = h_g(X)$, and $\phi'_{k'}(n') \equiv k'n'k'^{-1}$. Our goal isn't merely to show the two external-view constructions are isomorphic (we already know that), but rather to exhibit an $\alpha \in Iso(K', K)$ and $\gamma \in Iso(H, H')$ s.t. ϕ and ϕ' are related as in Prop 6.16. We have two obvious candidates: $\alpha = (h_g|_K)^{-1}$ (or, equivalently because of the SES-isomorphism relations, $\alpha = (q|_K)^{-1} \circ h_q^{-1} \circ (q|_{K'}))$ and $\gamma = h_n$. Let's see if these work. Let ϕ'' be the fully-transformed ϕ. I.e., $\phi''_{k'}(n') = \gamma(\phi_{\alpha(k')}(\gamma^{-1}(n')))$. This is just $\gamma(\alpha(k') \cdot \gamma^{-1}(n') \cdot \alpha(k')^{-1})$. Note that we cannot apply γ to each separately because the domains are incompatible (we only can apply γ to an element of $H = N$, which the conjugate expression is but not the individual components of it). The expression can be rewritten $h_n((h_g|_K)^{-1}(k') \cdot h_n^{-1}(h') \cdot ((h_g|_K)^{-1}(k'))^{-1})$ (where on the right end, one inverse is an isomorphism inverse and the other is a group-multiplicative inverse). Having moved ϕ to ϕ'' on H' and K', we now can compare apples with apples: specifically, ϕ' and ϕ''. Ideally, they are equal — but it also is fine if they are related by automorphisms of H' and K' via Prop 6.16. Note that $(h_g|_K)^{-1}(k')$ is just $h_g^{-1}(k')$ (since $k' \in h_g(K)$) and $h_n^{-1}(h') = h_g^{-1}(h')$ since $h_g|_N = h_n$. I.e., we have $h_n(h_g^{-1}(k') \cdot h_g^{-1}(h') \cdot h_g^{-1}(k')^{-1})$. *These* can be combined to $h_n(h_g^{-1}(k'h'k'^{-1}))$. But $k'h'k'^{-1} \in N'$, so $h_g^{-1}(k'h'k'^{-1}) = (h_g|_N)^{-1}(k'h'k'^{-1}) = h_n^{-1}(k'h'k'^{-1})$. We then have $\phi''_{k'}(n') = h_n(h_n^{-1}(k'h'k'^{-1})) = k'nk'^{-1}$. I.e., $\phi' = \phi''$. We don't need any automorphisms since they are actually equal.

- We thus have seen that (i) for a fixed H and K, any two ϕ's in the same PA-class correspond to isomorphic right-splitting SES's with the same RSG-class and (ii) for isomorphic right-splitting SES's with K's in the same RSG-class, we have isomorphic external-view constructions with the same H and K and ϕ's in the same PA-class. I.e., the freedom of ϕ modulo PA-class is the same as the freedom of right-splitting SES-isomorphism class modulo RSG-class. I.e., all three views stated this way have the same information content.
- Between these two propositions, we see that the PA-classes and RSG-classes really have the same information. To show that the remaining freedom in ϕ is the same as the remaining SES-view or internal-view freedom, let's show that the round-trips are identity. I.e., our procedures for going external-view to SES-view and back are inverses.

- **Prop 6.20:** If we start with an internal-view semidirect product, then map it to an external-view one via Prop 6.15 and them map it back via Prop 6.17 (which really means mapping it to an SES-view one via Prop 6.14 and then to an internal-view one via Prop 6.13), we get the same internal-view semidirect product (modulo the type of automorphism of Prop 6.11), or equivalently modulo the element of the RSG-class.

> Pf: Start with some (G, N, K) satisfying the internal-view requirements. Prop 6.15 maps this to external view (H', K', ϕ') given by $H' = N$, $K' = K$ and $\phi'_k(n) \equiv knk^{-1}$. We know that this $N \rtimes_{\phi'} K \approx G$. Prop 6.13) then maps this to an SES $e \rightarrow N \xrightarrow{i} N \rtimes_{\phi'} K \xrightarrow{q} K \rightarrow e$, where $i(n) = (n, e)$, $q(n, k) = k$ and the right-split subgroup is (e, K). Prop 6.11 then takes us back to $G'' = N \rtimes_{\phi'} K$, $N'' = (N, e)$, and $K'' = (e, K)$. $N'' \cap K'' = \{e\}$ trivially. From the SES, we already know that $(N \rtimes_{\phi'} K)/(N, e) \approx K$. Since the right-split subgroup of the SES is (e, K), the right-split map is $(q|_{e,K})^{-1}$. I.e., $j(k) = (e, k)$. Since $q|_{(e,K)}$ is an isomorphism, we do indeed have an internal-view. We thus end up with $G'' \equiv N \rtimes_{\phi'} K$, $K'' \equiv (e, K) \subset G''$, and $N'' \equiv (H, e) \triangleleft G'$. As seen in Prop 6.15, we can define an isomorphism $G'' \rightarrow G$ via $(n, k) \rightarrow n \cdot k$. This restricts to isomorphisms $(n, e) \rightarrow n$ and $(e, k) \rightarrow k$, thus recovering the original N and K. I.e., the resulting G'' is isomorphic to the original G in a way which restricts to isomorphisms between K'' and K and between N'' and N. We thus recover our original inner-product (SES-isomorphism) and RSG-class.

- **Prop 6.21:** If we start wth an external-view semidirect product, then map it to an internal-view one via Prop 6.17 (which really means mapping to the SES-view via Prop 6.14 and then to the internal-view via Prop 6.13) and then map it back to the external-view via Prop 6.15, we get what we started with (modulo the type of isomorphism described in Prop 6.10).

> Pf: We start with H, K, ϕ. Let $G \equiv H \rtimes_{\phi} K$. From Prop 6.14, this becomes the SES $e \rightarrow H \xrightarrow{i} G \xrightarrow{q} K \rightarrow e$, where $i(h) = (h, e)$ and $q(h, k) = k$, and the right-split map is $j(k) = (e, k)$ (with right-split group (e, K)). From Prop 6.13, we get the internal-view $G' \equiv G$, $N' \equiv (H, e)$, $K' \equiv (e, K)$. From Prop 6.15, we get the external-view $H'' \equiv N' = (H, e)$, $K'' \equiv K' = (e, K)$, and $\phi''_{k''}(h'') \equiv k''n''k''^{-1}$. From Prop 6.15 we also know we have an isomorphism $\gamma : G'' \rightarrow G'$ via $\gamma(h, k) \equiv hk$. However, $h \in N' = (H, e)$ and $k' \in K' = (e, K)$ and multiplication is in $G' = G$. I.e., it is $\gamma(h, k) = (h, e)(e, k)$ where the latter multiplication is in G'. But $G' = G$, so γ is an isomorphism between $H'' \rtimes_{\phi''} K''$ and $H \rtimes_{\phi} K$, given by $\gamma(h, k) = (h, e)(e, k) = (\phi_k(h), k)$ (since the multiplication takes place in $G' = G$). Note that we can write $H'' \rtimes_{\phi''} K'' = H \rtimes_{\phi''} K''$ because $\gamma|_{(H,e)} = Id_{(H,e)}$ and $\gamma|_{(e,K)} = Id_{(e,K)}$, so we end up with the same H and K we started with. Since $\gamma(h, k) = (h\phi_k(h), k)$. It may not look like it, but ϕ and ϕ' actually are the same. As mentioned earlier, $(e, k)(h, e)(e, k)^{-1} = (\phi_k(h), e)$ by applying the multiplication rule on G. I.e. $\phi_k(h)$ is just conjugacy of h by k. This isn't a surprise, since we built the multiplication on G so that it would be. However, it tells us that ϕ'' is just another way of writing ϕ. We thus get back exactly the original external-view semidirect product.

- Note that, from the definition of the direct product in the different views, we see that the direct product is just a type of semidirect product. In the external-view it has $\phi_k = Id_H$ for all $k \in K$, in the internal-view it has $K \triangleleft G$, and in the SES-view it left-splits.

There are a few important things to note about the semidirect product:

- The various semidirect products of H and K may be isomorphic to one another, but in general need not be. I.e., a given H and K may have multiple distinct semidirect products. This actually happens.

> Wikipedia mentions that there are 4 non-isomorphic semidirect products of C_8 and C_2 (the former being the normal subgroup in each case). One is a Direct Product, and the other 3 are not.

- It also is possible for a given group G to arise from several distinct semidirect products of different pairs of groups.

> Again from Wikipedia, there is a group of order 24 which can be written as 4 distinct semidirect products of groups.

- The multiplication defined in the external view may seem very strange and unintuitive. In essence, here is what's happening: for a direct product, H and K are independent of one another. Each half of the pair (h, k) acts only on its own group. For a semidirect product, the non-normal half (K) can twist the normal half (H). Each element of K can alter H in some prescribed fashion, embodied in $\phi(k)$. So K is unaffected by H but H can be twisted by K. This is directly evident in the (easily verified) conjugation relation $(e, k)(h, e)(e, k)^{-1} = (\phi_k(h), e)$.

- The basic idea of a semidirect product is similar to that of a fiber bundle. In the latter, a fiber twists (via a group of homeomorphisms) as we move around the base space. Here, the normal subgroup twists via automorphisms as we move around the non-normal part. Each generalizes a direct product (one of groups, the other of topological spaces) and measures our need to depart from it. The two are closely related, but this relationship will be discussed in a different set of notes.

- Prop: A semidirect product of two groups is abelian iff it is a direct product and the subgroups are abelian.

Pf: This is easiest seen in the internal-view. If G is abelian, every subgroup is normal (since $gkg^{-1} = k$ for all $g \in G$ and $k \in K$) so we have a direct product. Every subgroup of an abelian group also is abelian. Going the other way, a direct product is a semidirect product where K happens to be normal. A direct product of abelian groups trivially is abelian.

See `https://math.stackexchange.com/questions/425062/can-the-semidirect-product-of-two-groups-be-abelian-group` for discussion.

7 Group Extensions

We saw that a direct product is a particular type of semidirect product, one in which (i) ϕ maps all of K to Id_H (external view), or (ii) both N and Q are normal subgroups of G (internal view), or (iii) the SES left-splits rather than just right-splitting (SES-view). Similarly, a semidirect product is a particular type of group extension.

Group extensions are the most general form of this type of construction, and similarly can be described in terms of an external view, an internal view, and an SES view. In fact, a more efficient treatment of the subject would have begun by defining group extensions, deriving the associated multiplication and properties (as we do in the addendum), and only then discussing the special cases which correspond to semidirect products and direct products.

However, efficiency need not comport well with clarity. Most physicists are intimately familiar with direct products and have some interaction with semidirect products (whether aware of it or not) but have little experience with general group extensions. The point of these notes is to remedy this, not to provide a maximally concise treatment for mathematicians.

To this end, we began by reviewing general topics such as normal subgroups and short exact sequences, then proceeded to the familiar cases of direct products and semidirect products, and finally arrived at general group extensions. In doing so, there has been much replication of effort. However, that is a small cost for comprehensibility.

A group extension is:

- External view: A general way of constructing a group from two other groups in a manner which creates a normal/quotient relationship. We'll see the explicit form of this momentarily.
- Internal view: A general normal/quotient relationship.
- SES view: An SES-isomorphism class.

As with semidirect products, the three views are the same up to SES-isomorphism. We'll interpret "general" in the external view and internal view as meaning isomorphic in a way where the isomorphisms are compatible. Since this always comes down to (and is more elegantly expressed as) SES-isomorphism, we'll just call it that, even in the context of the two other views.

The term "group extension" variously is used by people to refer to an individual SES, an isomorphism class of SES's, a core normal/quotient SES, the group B in an SES, and the isomorphism class of group B in an SES.

Given an SES $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$, people generally say that B is an "extension of C by A". However, some people adopt the opposite usage and say B is an "extension of A by C". See `https://terrytao.wordpress.com/2010/01/23/some-notes-on-group-extensions/` for a discussion of some such conventions.

The equivalence of the three views is *mostly* trivial in light of results we've already discussed involving SES's and normal/quotient relationships, but we'll state them below anyway.

However, first we must formalize the external view. The explicit construction of the multiplication on a group extension is a bit involved, so we'll relegate that to the addendum. At present, we'll just state the result obtained there.

- **Prop 7.1:** : Let H and K be groups and let $\eta : K \to Aut(H)$ and $\nu : K \times K \to H$ be maps (not homomorphisms) s.t. (a) $\eta(e) = Id_H$, (b) $\nu(k,e) = \nu(e,k) = e$ for all $h \in H$, (c) $\eta_k(\nu(k',k'')) \cdot \nu(k,k'k'') = \nu(k,k') \cdot \nu(kk',k'')$ for all $k,k',k'' \in K$, and (d) $\eta_k(\eta_{k'}(h)) = \nu(k,k') \cdot \eta_{kk'}(h) \cdot \nu(k,k')^{-1}$ for all $k,k' \in K$ and $h \in H$. Given these elements, we can construct a group G s.t.

  Note that some of the listed items are direct consequences of one another. We're just listing various relevant properties of our construction.

  - (i) The elements of G are labeled (but not necessarily parametrized) by (h,k).
  - (ii) $(H,e) \triangleleft G$.
  - (iii) $i(h) = (h,e)$ is an isomorphism $H \to (H,e)$.
  - (iv) $K \approx G/(H,e)$.
  - (v) $g(h,k) = k$ is a surjective homomorphism $G \to K$ s.t. ker $g = (H,e)$.
  - (vi) $(h,k) \cdot (h',k') \equiv (h \cdot \eta_k(h') \cdot \nu(k,k'), kk')$ is the multiplication.
  - (vii) (e,e) is the multiplicative identity.
  - (viii) $(h,k)^{-1} = ({\eta_k}^{-1}(h^{-1} \cdot \nu(k,k^{-1})^{-1}), k^{-1})$ is the inverse (where ${\eta_k}^{-1}$ is the inverse of the automorphism η_k).

    Note that ${\eta_k}^{-1}$ is *not* the same as η_{k-1} because $\eta : K \to Aut(H)$ is not a homomorphism.

    This also can be written $({\eta_k}^{-1}(\nu(k,k^{-1}) \cdot h)^{-1}, k^{-1})$.

For now, the key takeaway is the multiplication (vi). This looks similar to the semidirect product except that η (the counterpart of the semidirect product's ϕ) no longer is a homomorphism and we also have a map ν along with some weird conditions on their interplay. Basically, ν tells us how much we deviate from being a semidirect product. It is the obstruction to the SES right-splitting.

The "external view" of a group extension is precisely the construction just described (and fleshed out in the addendum). I.e., we are given a suitable H, K, η, and ν, and we construct G and the attaching maps i and γ.

In terms of this construction, we immediately see that:

- Semidirect product: A semidirect product defined by (external-view) (H,K,ϕ) is a group extension with (external-view) $\eta = \phi$ (now a homomorphism) and ν trivial (i.e. $\nu(k,k') = e$ for all $k,k' \in K$).
- Direct product: ν again is trivial, and η now is too. Specifically, $\eta_k = Id_H$ for all $k \in K$.

As mentioned, most of the equivalence of the three views has already been established in our earlier discussion, but one has not. For completeness, let's now list them.

- **Prop 7.2:** : An SES-view group extension gives rise to an internal-view one.

Pf: We saw in Prop 3.8 and Prop 3.13 that an SES $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$ is isomorphic to its derived SES's, including its core normal/quotient SES. I.e., each SES gives rise to an internal-view group extension via $f(A) \triangleleft B$. Different SES's in the isomorphism class may have different core normal/quotient SES's but the latter all are SES-isomorphic. I.e., $N \approx N'$ and $G \approx G'$ and $G/N \approx G'/N'$ *and* we can pick three compatible isomorphisms. This compatibility is just SES-isomorphism between the corresponding core normal/quotient SES's, and is best expressed that way even in the context of the internal-view.

- **Prop 7.3:** : An internal-view group extension gives rise to an SES-view one.

Pf: From Prop 3.13 we know that all SES's with $N \triangleleft G$ as its core normal/quotient relation are SES-isomorphic. We then can expand to the entire SES-isomorphism class. Every choice of $N' \triangleleft G'$ s.t. $N' \approx N$ and $G' \approx G$ and $G'/N' \approx G/N$ in a compatible way just gives rise to an SES-isomorphic core normal/quotient SES.

- **Prop 7.4:** : An external-view group extension gives rise to an internal-view one.

Pf: From Prop 7.1, $(H, e) \triangleleft G$. We then extend both sides to SES-isomorphism classes, of course.

- **Prop 7.5:** : An external-view group extension gives rise to an SES-view one.

Pf: From Prop 7.1, $(H, e) \triangleleft G$. This gives rise to a core normal/quotient SES, which we then extend to an SES-isomorphism class. Equivalently, we could define the SES $e \to H \xrightarrow{i} G \xrightarrow{\gamma} K \to e$, with G the group resulting from the construction of Prop 7.1 and with $i(h) = (h, e)$ the inclusion map and $\gamma(e, k) = k$ the combined quotient/attaching map for K, and then expand this SES to an SES-isomorphism class.

- **Prop 7.6:** An internal-view group extension gives rise to an external-view one.

Pf: Given $N \triangleleft G$, we define $H \equiv N$ and $K \equiv G/N$. To come up with η and ν, we'll use some of the tactics from the addendum. Pick a section u (i.e. $u : G/N \to G$ s.t. $q \circ u = Id_{G/N}$) s.t. $u(e) = e$. Note that u is a map, not a homomorphism (if it was a homomorphism, we would have a semidirect product). Define $\eta_k(h) \equiv u(k) \cdot h \cdot u(k)^{-1}$ and $\nu(k, k') \equiv u(k) \cdot u(k') \cdot u(k \cdot k')^{-1}$ (where all the multiplication takes place in G and G/N, which we are given). To see that η is a map $K \to Aut(H)$, we observe that η_k is the restriction of an inner-automorphism of G to H and thus is an automorphism of H (since H is normal in G). To see that $\nu(k, k') \in H$, we'll show that $q(\nu(k, k')) = e$. $q(u(k)u(k')u(kk')^{-1}) = q(u(k))q(u(k'))q(u(kk'))^{-1}$ because q is a homomorphism, but $q \circ u = Id_K$, so this is just $k \cdot k' \cdot (kk')^{-1} = e$. Therefore, $\nu(k, k') \in q^{-1}(e) = H$. Next, let's confirm that the requirements (a-d) of Prop 7.1 are satisfied. (a) Since $u(e) = e$, $\eta_e = Id_H$ trivially. (b) $\nu(k, e) = u(k)u(e)u(k \cdot e)^{-1} = u(k)u(k)^{-1} = e$ and ditto for $\nu(e, k)$. (c) $\eta_k(\nu(k', k'')) \cdot \nu(k, k'k'') = u(k)u(k')u(k'')u(k'k'')^{-1}u(k)^{-1}u(k)u(k'k'')u(kk'k'')^{-1}$, which reduces to $u(k)u(k')u(k'')u(kk'k'')^{-1}$. On the other hand, $\nu(k, k')\nu(kk', k'') = u(k)u(k')u(kk')^{-1}u(kk')u(k'')u(kk'k'')^{-1}$, which also reduces to $u(k)u(k')u(k'')u(kk'k'')^{-1}$. (d) $u(k)u(k')hu(k')^{-1}u(k)^{-1}$ on the left and $\nu(k, k')u(kk')hu(kk')^{-1}\nu(k, k')^{-1}$ on the right. The latter expands to $u(k)u(k')u(kk')^{-1}u(kk')hu(kk')^{-1}u(kk')u(k')^{-1}u(k)^{-1}$, which reduces to $u(k)u(k')hu(k')^{-1}u(k)^{-1}$. We thus have satisfied all the prerequisites, and Prop 7.1 constructs a group G', whose elements are labeled via (h, k). Define $h_g : G' \to G$ via $h_g(h, k) \equiv h \cdot u(k)$. Then $h_g(e, e) = e$ (since $u(e) = e$) and $h_g((h, k)(h', k')) = h_g((h\eta_k(h')\nu(k, k')), kk') = h\eta_k(h')\nu(k, k')u(kk') = hu(k)h'u(k)^{-1}u(k)u(k')u(kk')^{-1}u(kk') = hu(k)h'u(k')$. On the other hand, $h_g(h, k)h_g(h', k') = hu(k)h'u(k')$. So $h_g((h, k)(h', k')) = h_g(h, k)h_g(h', k')$ and we have a homomorphism. To see that h_g is injective, first observe that if $hu(k) = h'u(k')$ then $q(hu(k)) = q(h'u(k'))$ so $q(h)q(u(k)) = q(h')q(u(k'))$ and $e \cdot k = e \cdot k'$, so $k = k'$. But then $u(k) = u(k')$ so $h = h'$. To see that h_g is surjective, pick a g. Let $q(g) = k$ and let $h = g \cdot u(k)^{-1}$ (which is in H since $q(g \cdot u(k)^{-1}) = q(g) \cdot q(u(k)^{-1}) = k \cdot k^{-1} = e$). [Note that $u(k)^{-1}$ and $u(k^{-1})$ are in the same coset but need not be the same element. We only used the former.] Then $g = h \cdot u(k)$. So h_g is a bijective homomorphism and thus an isomorphism. $h_g(h, e) = h$ and $h_g(e, k) = u(k)$. This is an SES-equivalence (i.e. $h_n = Id_N$ and $h_q = Id_{G/N}$). Why the latter when we have $h_g(e, k) = u(k)$? Because K just labels the group G/N and (e, K) just labels the quotient group $G'/(H, e)$. Viewed as the same group (i.e. $(e, K) = K$), the relevant $h_q : K \to K$ is given by Id_K. Bearing in mind that h_g takes us from G' to G (the opposite of our usual convention), this makes the quotient commute: $q \circ h_g = h_q \circ q'$, which becomes $q(h_g(h, k)) = h_q(q'(h, k))$. The right side is $Id_K(k) = k$ and the left side is $q(hu(k)) = q(h)q(u(k)) = ek = k$. So we have an SES-equivalence and the external-view construction does indeed correspond to our internal-view one.

Note that the choice of section u is arbitrary. We'll see in the addendum that a different u' gives a different η' and ν', and the same multiplication on the constructed G' looks quite different in terms of these. However, that does not apply here. We are choosing a section of G, not of our constructed G', and *then* constructing G' and showing SES-equivalence. Put another way, we can think of each choice of u as a choice of labeling for pts in G via (h, k). The coset always is labeled with the relevant k, so that's the same regardless of our choice of u. Within each coset, we don't have complete latitude to label elements (via the h part of the (h, k) pair), but rather may choose a single reference element to correspond to (e, k). I.e., we have a choice of section of G. We then *define* this section to be labeled (e, k) and the rest follows.

- **Prop 7.7:** An SES-view group extension gives rise to an external-view one.

Pf: We just use Prop 7.2 to go to the internal-view and Prop 7.6 to go to the external view.

7.1 Central Extensions Revisited.

We earlier defined a "central" extension in terms of SES's. As we now know, an SES is just a group extension, so the reason for the name should be clear. Let's consider the definition from the three vantage points.

- SES-view: A central extension was defined as an SES $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$ where $f(A)$ not only is normal in B but lies in its center (i.e. $f(A) \subseteq Z(B)$). Obviously, this requires that A be abelian.
- Internal-view: A central extension is a normal/quotient relation in which N is in the center of G (i.e., $N \subseteq Z(G)$). This constrains G/N, of course.
- External-view: A central extension is constructed from H and K just like for an ordinary group extension, but with the further constraint during construction that $(H, e) \subseteq Z(G)$. Obviously, this requires that H be abelian. It also constrains the admissible η and ν.

  Every η and ν which satisfy the original constraints of the theorem give rise to a group extension. However, only some (or none) of these give rise to central extensions. For a central extension, $\eta_k = Id_H$ for all $k \in K$ (since $u(k)hu(k)^{-1} = u(k)u(k)^{-1}h$ for $h \in H \subseteq Z(G)$). The first constraint becomes $\nu(k', k'')\nu(k, k'k'') = \nu(k, k')\nu(kk', k'')$ and the 2nd is trivially satisfied. We thus can say that if H is abelian and we are given a $\nu : K \times K \to H$ s.t. $\nu(k, e) = \nu(e, k) = e$ and $\nu(k', k'')\nu(k, k'k'') = \nu(k, k')\nu(kk', k'')$ we have a central extension (with η automatically generated as trivial) via our construction.

7.2 Classification of Group Extensions

One key problem is to identify all the group extensions of C by A (or possibly of C by anything). I.e., we want to classify the distinct SES-isomorphism classes of the form $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$ (or possibly of the form $e \to \mathit{Anything} \xrightarrow{f} B \xrightarrow{g} C \to e$).

It turns out this can be done via the 2nd (in the case of central extensions) or 2nd and 3rd (in the case of general extensions) group cohomologies. Group cohomology is a cohomology theory, but a non-topological one. This is a topic for another time, but here's a brief summary.

Given a group G, a left G-module M is an abelian group (ex. a free abelian group generated from some set) along with a group action of G on M. I.e., it's like an ordinary module, but instead of coefficients drawn from a ring they are drawn from a group. Since, unlike a ring, the group G need not be abelian, this is a generalization of an R-module. Given a G-module M, define $C^n(G, M)$ to be the abelian group of all fns from $G^n \to M$..

I.e. $C^n(G, M)$ consists of all fns of the form $f(g_1, \ldots, g_n)$ producing values in M. It is an abelian group under the operation $(f + g)(g_1, \ldots, g_n) \equiv f(g_1, \ldots, g_n) + g(g_1, \ldots, g_n)$, where the right-side addition is in M.

We can define a purely algebraic map $d^{(n+1)} : C^n(G, M) \to C^{(n+1)}(G, M)$ which satisfies $d^{(n+1)} \circ d^n = 0$. This is a cochain complex, and thus gives rise to a cohomology theory via $H^n(G, M) \equiv \ker d^{(n+1)}/\mathrm{Im}\ d^n$. It is these cohomology groups which are encountered when classifying SES's, rather than anything topological.

We say "cochain complex" and "cohomology theory" rather than "chain complex" and "homology theory" solely because of the notational direction of the arrows d. This affects nothing, and is merely a matter of nomenclature.

Explicitly, d is defined as follows. Given fn $\phi : G \times \cdots (ntimes) \cdots \times G \to M$ (i.e. $\phi \in C^n(G, M)$), we define $(d^{n+1}\phi)(g_1, \ldots, g_{n+1}) \equiv g_1\phi(g_2, \ldots, g_{n+1}) + \sum_{i=1}^{n}(-1)^i\phi(g_1, \ldots, g_{i-1}, g_ig_{i+1}, g_{i+2}, \ldots, g_{n+1}) + (-1)^{n+1}\phi(g_1, \ldots, g_n)$. Note that $(-1)^i$ is shorthand for $+$ or $-$ (addition of what follows or of its additive-inverse) according to whether i is even or odd. There is no multiplicative unit element 1 in M (it is not a group under multiplication).

- If H is abelian then $H^2(K, H)$ classifies the (isomorphism classes of) central extensions of K by H.
- $H^2(K, Z(H))$ and $H^3(K, Z(H))$ together can be used to classify the (isomorphism classes of) general extensions of H by K.

  The 2nd applies even if H is abelian (and thus $Z(H) = H$). It is quite possible to have abelian non-central extensions of K by H. In that case, $H^2(K, H)$ classifies the central extensions but we also need $H^3(K, H)$ to classify the non-central extensions.

  Note that we're quietly upgrading H or $Z(H)$ to a G-module here and have glossed over a great deal. This is a very quick summary and not meant to be thorough. We'll return to this topic in excruciating detail in a future post.

The study of SES's and group extensions (as well as group cohomology) isn't found in most algebra textbooks. It tends to appear in treatments of "homological algebra", though often obscured by category-theory jargon and notation involving "tor" and "ext" functors, etc.

For the general case, the details are spelled out in Eilenberg and Maclane's original paper "Cohomology Theory in Abstract Groups. II: Group Extensions with a non-Abelian Kernel", Annals of Mathematics, Vol 48, No. 2, Apr, 1947.

8 Summary: Direct Products, Semidirect Products, and Group Extensions

Let's review the status of these three constructions from the three viewpoints we've discussed. As we saw, the direct product is unique and a type of semidirect product, and each semidirect product is a type of general group extension.

The external view involves construction of a group G from groups H and K. This can be regarded as an operation.

- Direct Product: $G = H \oplus K$ is the obvious pairwise construction.
- Semidirect Product: $G = H \rtimes_\phi K$ constructed using homomorphism ϕ. There may be multiple of these, corresponding to different ϕ's.
- Group Extension: A group G, constructed as set out in the addendum using suitable maps η and ν. There may be multiple of these, corresponding to different η's and ν's.

The internal view considers the relationship between an existing group G and one or more normal subgroups.

- Direct Product: $G = N_1 \oplus N_2$ involves two disjoint normal subgroups such that $G = N_1 N_2$.
- Semidirect Product: $G = N \rtimes K$ involves a normal subgroup $N \triangleleft G$ and a disjoint subgroup $K \subset G$ s.t. $G = NK$.
- Group Extension: Involves just a single normal subgroup $N \triangleleft G$.

The SES view considers three groups related by an SES.

- Direct Product: An SES that left-splits (and thus also right-splits).
- Semidirect Product: An SES that right-splits.
- Group Extension: An SES.

We're being loose in our descriptions here. As we saw, these definitions technically involve SES-isomorphism classes. We can caveat each definition via "modulo SES-isomorphism".

9 Addendum: The Multiplication in a Group Extension

We'll somewhat follow the treatment in The Encyclopedia of Math at `https://encyclopediaofmath.org/wiki/Extension_of_a_group`.

We saw that a group extension is just an SES-isomorphism class. Let's consider two distinct but equivalent (modulo SES-isomorphism) questions:

- Q1: Given groups A and C, how can we construct a SES $e \to A \xrightarrow{f} B \xrightarrow{g} C \to e$? I.e., what choices of B, f, and g would give us one?

  > We also may wish to know (i) which choices lead to isomorphic B's and (ii) which subset of these choices lead to equivalent SES's. Note that this isn't the difference between isomorphic and equivalent SES's. As discussed earlier, it is quite possible to have the same A and C and isomorphic B's (call them B and B'), but not an SES-isomorphism (let alone SES-equivalence) because no isomorphism between B and B' makes the diagram commute. We thus have three situations in which $B \approx B'$: (i) there may be an isomorphism $\alpha : B \to B'$ s.t. $f' = \alpha \circ f$ and $g = g' \circ \alpha$, in which case we have an SES-equivalence, (ii) this may be too strict but there may be automorphisms h_a and h_c and an isomorphism $h_b : B \to B'$ s.t. $f' \circ h_a = h_b \circ f$ and $g' \circ h_b = h_c \circ g$, in which case we have an SES-isomorphism, (iii) there may be no h_a, h_b, and h_c which make the diagram commute, in which case $B \approx B'$ but there is no SES-isomorphism or SES-equivalence.

- Q2: Given any H and K, how can we construct a group G where H is isomorphic to a normal subgroup of G and K is isomorphic to the corresponding quotient group?

Up to SES-isomorphism, Q1 is the same as asking how many ways we can build a core normal/quotient SES. We then can obtain any other SES in the isomorphism class via attaching maps to one of those core normal/quotient SES's. Q2 is in fact answered by addressing this very form of Q1. We'll use the latter notation.

First, let's map out the basic structure of G.

- **Prop 9.1:** The normal/quotient relationship requires that setwise $G = H \times K$. I.e., the points in G can be labeled (h, k).

  > But bear in mind our earlier warnings about labeling vs parametrizations. This is just a labeling. We are making no claims about G resembling $H \times K$ topologically or in any other regard.

  > Pf: Given any group G and $N \triangleleft G$, G setwise is $\cup_{i \in G/N} N$. I.e., setwise G consists of $|G/N|$ copies of N (one for each coset). We're just using k to label the cosets and h to label the point in the coset (*but* with no cross-coset uniformity of meaning to this h label!). All the meaning will be expressed through our definition of multiplication on G.

- We'll earmark the set (H, e) as our normal subgroup and accordingly choose the attaching map f to be the inclusion $i(h) = (h, e)$.

  > Since we're labeling the cosets by k, we're just picking (H, e) as the identity coset. Of course, we'll have to ensure that any multiplication we pick on G will make (H, e) normal in G. This will constrain us, but we would be equally constrained if we chose some other subset of G to be normal. I.e., we lose no generality, and this is just a convenient labeling.

- **Prop 9.2:** The constraint that i be an injective homomorphism to G (under whatever multiplication we impose on G) implies that the full group multiplication on (H, e) is defined by (e, e) being the identity and $(h, e)(h', e) = (hh', e)$.

  > Pf: This just follows from the definition of a homomorphism. i trivially is injective from H to G, and its image is (H, e), so it is an isomorphism to (H, e). Therefore, (H, e) must have the same exact multiplication as H.

  - **Prop 9.3:** (H, e) is a subgroup of G, and $(h, e)^{-1} = (h^{-1}, e)$.

    > Pf: We could just use the fact we're isomorphic to H, but let's do it explicitly. Let $(h, e)^{-1} = (h', e)$. Then $(hh', e) = (e, e)$, so $h' = h^{-1}$.

- **Prop 9.4:** Given the construction so far, the identity on G is (e, e).

  > Pf: $i(e) = (e, e)$ must be the identity on (H, e) since i is a homomorphism from H to (H, e) Suppose there is some $(h, k) \in G$ s.t. $(h, k)(h', k') = (h', k')$ for all (h', k') (i.e. (e, e) doesn't extend as the identity to all of G). Obviously, $k \neq e$ or we'd have two identities in (H, e). What about outside of (H, e)? That won't work either. By (ii), (H, e) is required to be a subgroup of G. The identity on G must be an element of every subgroup of G.

- **Prop 9.5:** Given the constraints (i) $(H, e) \triangleleft G$ and (ii) $K \approx G/(H, e)$ under whatever multiplication we adopt for G, we can define a surjective homomorphism $\gamma : G \to K$.

  > Pf: Suppose we are given a multiplication on G for which those two conditions hold. Since $K \approx G/(H, e)$, $\exists$ an isomorphism $\alpha : G/(H, e) \to K$. Any such α indexes our cosets by K. Let q be the canonical quotient homomorphism $G \to G/(H, e)$. Define $\gamma : G \to K$ to be $\alpha \circ q$. Of course, different choices of α give different γ's. Note that this whole construction depends on the multiplication we impose on G. We're just deriving a consequence of the constraints on that multiplication.

- **Prop 9.6:** $(H, e) \triangleleft G$ is equivalent to the existence of a surjective homomorphism $\gamma : G \to K$ with $\ker \gamma = (H, e)$.

Pf: Given a multiplication on G s.t. $(H, e) \triangleleft G$, ker $q = (H, e)$ by the definition of the quotient homomorphism $q : G \to G/(H, e)$. The kernel of any isomorphism $\alpha : G/(H, e) \to K$ is e, so ker $\gamma =$ ker $q = (H, e)$ holds regardless of the specific choice of α (and thus γ). Going the other way, given a surjective homomorphism γ with ker $\gamma = (H, e)$, the First homomorphism thm tells us that ker $\gamma \triangleleft G$, so $(H, e) \triangleleft G$.

It is important to observe here that, unlike (H, e), the set (e, K) is *not* a subgroup of G in general. We certainly have a bijective map $K \to (e, K)$. But it is not a homomorphism in either direction. γ is a homomorphism from G to K, but it need not restrict to a homomorphism on (e, K). To do so, we not only need some section of G to be a copy of K (i.e. we need a semidirect product) but that this section happens to be (e, K). As we will see, our multiplication on $(h, k)(h', k')$ will end up taking the form $(something, kk')$. This may seem to contradict what we just said about not necessarily having a copy of K in G, but it actually doesn't. A copy of K exists iff $(e, k)(e, k') = (e, kk')$ for all k, k'. Though the 2nd element is indeed kk', the first need not be e. I.e. $(e, k)(e, k') = (not - e, kk')$ in general. In the case of a semidirect product it is e (since $(e, k)(e, k') = (e\phi_k(e), kk') = (e, kk')$). For a general group extension it is not. This is a very important distinction to keep in mind. Again, γ is a homomorphism $G \to K$, but does not restrict to one on $(e, K) \to K$ because (e, K) is not necessarily a subgroup of G. This will be apparent as we proceed with the construction.

- **Prop 9.7:** The cosets are of the form (H, k).

Pf: Since we have an isomorphism (and hence bijection) between the group of cosets (i.e. $G/(H, e)$) and K, the cosets are labeled by elements of K. Of course, this doesn't mean α maps (H, k) to k. We've used K (along with H) for labeling points in the group G we are constructing but have imposed no constraint on how they match up to the elements of the group K. All we really have said is that the quotient relation slices G into things of the form (H, k). Different α's will match them up in different ways, and none need project out the second element (i.e. map (H, k) to k). Put another way, $\gamma(h, k)$ need not equal k. Nor need there exist an automorphism on K which fixes this. However, this is a specious concern because our labeling of cosets is arbitrary to begin with. We're free to choose a labeling that suits our needs and makes the labels align for whatever choice of α we employ.

- **Prop 9.8:** We always can choose, without loss of generality, $\gamma(h, k) = k$ as our SES homomorphism.

Pf: We saw that the cosets are of the form (H, k) but that the homomorphism α need not take (H, k) to k. However, the k in (h, k) is just a label. We can relabel things so that the coset labels *do* match up. This changes the labeling of the multiplication of elements in G — but crucially does not affect multiplication on (H, e) or the normality of (H, e) relative to the multiplication. I.e., we always can choose our labeling so that each coset $[k]$ is labeled by k rather than some other k'. We lose no generality doing so. Note that this choice of labeling and γ corresponds to the obvious $\alpha : G/(H, e) \to K$ given by $\alpha([k]) = k$.

Note that for any choice of α, there is a labeling which makes things match up — but it differs between α's. If we pick a different α, our results are related by an automorphism of K. The core normal/quotient relation is unaffected but the labeling no longer aligns. We can choose our labelings to be whatever we want (they needn't be related by automorphisms or anything else). Those for which an α exists s.t. $\alpha([k]) = k$ are related by automorphisms of K. In those cases, choosing that α simplifies the notation a lot. However, we may still use a different α or a labeling which has no associated α. This is perfectly valid, but makes the bookkeeping very messy.

Since we can do so without loss of generality, we'll assume we've chosen a labeling of cosets for which there is an associated α and that we are using this α and its $\gamma = \alpha \circ q$. I.e., $\alpha([k]) = k$ and $\gamma(h, k) = k$.

- **Prop 9.9:** Given our choices so far, the multiplication on G must be of the form $(h, k)(h', k') = (m(h, k, h', k'), kk')$ for some function m, and the inverse on G must be of the form $(h, k)^{-1} = (j(h, k), k^{-1})$ for some function j.

Pf: The most general conceivable form for multiplication is $(h, k)(h', k') = (m_1(h, k, h', k'), m_2(h, k, h', k'))$. As mentioned, the cosets are of the form (H, k) and we chose (without loss of generality) our labeling so that α has the form $\alpha([k]) = k$. With this labeling, the multiplication on the cosets matches that on K (via label) directly. I.e. $\gamma((h, k)(h', k')) = \gamma(h, k) \cdot \gamma(h', k') = k \cdot k'$. But $\gamma((h, k) \cdot (h', k')) = \gamma(m_1(h, k, h', k'), m_2(h, k, h', k')) = m_2(h, k, h', k')$. So $m_2(h, k, h', k') = k \cdot k'$. The most general form of the inverse is $(h, k)^{-1} = (j_1(h, k), j_2(h, k))$. By similar reasoning, $\gamma((h, k)^{-1}) = \gamma(h, k)^{-1} = k^{-1}$. But $\gamma((h, k)^{-1}) = \gamma(j_1(h, k), j_2(h, k)) = j_2(h, k)$, so $j_2(h, k) = k^{-1}$.

- Let's summarize the general landscape for G so far:
  - Setwise $G = H \times K$
  - We then ask what multiplications we can impose on G s.t. H is isomorphic to some normal subgroup of G and K is isomorphic to the corresponding quotient group. We do so by assuming a multiplication on G and then determining the necessary consequences.
  - Our SES "f" map is chosen (without loss of generality) to be $i(h) = (h, e)$, declaring our normal subgroup to be (H, e).
  - i is an isomorphism $H \to (H, e)$, from which we know the multiplication on (H, e) as a subgroup of G.
  - (e, e) is the identity on G.
  - The cosets are labeled by (H, k) (but not necessarily with the label k matching up to the corresponding $k \in K$ under any isomorphism).

  - Our normality requirement amounts to $\ker\gamma = (H,e)$ (for the SES map γ), where $\gamma = \alpha\circ q$ (for q the quotient map $G \to G/(H,e)$ any isomorphism $\alpha : G/(H,e) \to K$).
  - For any choice of isomorphism α, our SES "g" map is chosen (without loss of generality) to be $\gamma(h,k) = k$.
  - For any isomorphism $\alpha : G/(H,e) \to K$ there is a coset-labeling s.t. $\alpha([k]) = k$ (and thus $\gamma(h,k) = k$). Whatever α we pick, we'll assume this associated labeling.
  - $(h,k)(h',k') = (something, kk')$
  - $(h,k)^{-1} = (something, k^{-1})$.

What about the dependence on α? It turns out this makes no difference.

Prop 9.10: If we choose a different α, the resulting group extension is SES-isomorphic.

Pf: We could go through a lot of rigamarole to exhibit a specific isomorphism, but there is no need. Any two isomorphisms α and α' are related by an automorphism on K. We saw earlier that such an attaching map doesn't change the core normal/quotient SES. More formally, we have an SES-isomorphism (not SES-equivalence) with the same H, K, G, and i. Only the γ's differ (and crucially, their kernels do not). So pick $h_h = Id_H$, $h_g = Id_G$, and $h_k = \gamma'\circ\gamma^{-1} = \alpha'\circ\alpha^{-1}$. The diagram trivially commutes.

We've now come as far as we can without picking a specific section of G. Recall that a section of G is a choice of representative from each quotient class in $G/(H,e)$. Let u be such a section. Since the classes of $G/(H,e)$ are labeled (via our assumption that the labeling matches the choice of α) by the corresponding elements of K, u can be written as a map $u : K \to G$ s.t. $\gamma\circ u = Id_K$.

Technically the "section" is a map $u' : G/(H,e) \to G$ s.t. $q\circ u' = Id_{G/(H,e)}$, and u is $u'\circ\alpha^{-1}$. However, this is just a matter of nomenclature and doesn't matter to us here — especially since our α is trivial due to our choice of labeling. We'll just refer to u as a "section".

Bear in mind that u is a map, not a homomorphism. In fact, there is no choice of u which is a homomorphism unless the SES splits (i.e. we have a semidirect product). We'll be measuring the deviation of u from being a homomorphism, aka the deviation of G from being a semidirect product.

Also note that our construction is purely algebraic. Unlike for a fiber bundle, there are no notions of "local" vs "global" sections here.

- For convenience, we'll sometimes write N for (H,e) from now on.

- Given a section u, we have a map $\eta : K \to Aut(N)$, given by $\eta_k(h,e) = u(k)\cdot(h,e)\cdot u(k)^{-1}$.

  - In our earlier notation, $\eta_k = \phi_{u(k)}|_N$. As discussed, it is an inner-automorphism of G but just an automorphism of (H,e) — and that only because we're requiring $(H,e) \triangleleft G$).
  - Note that we have several maps involving automorphism-like things:

    * The natural homomorphism $G \to Aut(N)$ given by the conjugation maps restricted to N. We called this α in our earlier discussion of groups (not to be confused with our current usage of α for an isomorphism $G/N \to K$). It takes $g \to \phi_g|_N$. This is independent of u.
    * The induced quotient homomorphism $G/N \to Out(N)$ given by $[x] \to [\phi_x|_N]$ (where we bear in mind that $\phi_x|_N$ is an element of $Aut(N)$, not $Inn(N)$ — so it isn't in the identity class of $Out(N)$). We called it β in our earlier discussion. We can pull this back to $K \to Out(N)$ using the isomorphism $\alpha^{-1} : K \to G/N$. This is independent of u.
    * When we pick a section u, we also have the map $\eta : K \to Aut(N)$. Each such η_k is an automorphism on N, but the set of them is *not* a homomorphism for the same reason (and in fact because) u is not. I.e. $\eta_{kk'} \neq \eta_k\circ\eta_{k'}$ and $\eta_{k^{-1}} \neq \eta_k^{-1}$ (map inverse) in general.

- Without loss of generality, we can constrain ourselves to sections with $u(e) = (e,e)$.

  There is no loss of generality because we can multiply any existing section u by a constant element $u(e)^{-1}$ to get a section with $u'(e) = (e,e)$.

  It may be tempting also to require $u(k^{-1}) = u(k)^{-1}$. However, this *does* lose us generality because we cannot bijectively construct such a section from any section.

- Let's denote the deviation of u from homomorphism by ν. Specifically: $u(k)u(k') = \nu(k,k')u(kk')$. We'll often write this as $\nu(k,k') = u(k)u(k')u(kk')^{-1}$.

  I.e., for a homomorphism, $\nu(k,k') = e$ for all k, k'.

- **Prop 9.11:** $\nu(k,k') \in (H,e)$.

  Pf: Because γ is a homomorphism, $\gamma(u(k)u(k')) = \gamma(u(k))\gamma(u(k')) = kk'$ and $\gamma(\nu(k,k')u(kk')) = \gamma(\nu(k,k'))\gamma(u(kk')) = \gamma(\nu(k,k')) \cdot (kk')$. Since the two are equal, $\gamma(\nu(k,k')) = e$, so $\nu(k,k') \in \ker\gamma = (H,e)$.

- Since $\eta_k \in Aut(N)$, we'll often treat it as in $Aut(H)$ and write $\eta_k(h)$ for $i^{-1} \circ \eta_k \circ i$. The context will make the choice clear. If it multiplies elements of H it is the latter, if it multiplies elements of G it is the former.

- Since $\nu(k,k') \in (H,e)$, we'll often treat it as in H. I.e., we'll write it for $i^{-1}(\nu(k,k'))$. The context will make the choice clear. If it multiplies elements of H it is the latter, if it multiplies elements of G it is the former.

- Some people write ${}^{k}h$ for $\eta_k(h,e)$. As with η_k, the dependence on the section is implicit. This can lead to confusing expressions, such as $h_1{}^{k}h_2$ for $h_1 \cdot \eta_k(h_2)$. We won't use this notation.

We've imposed our SES (i.e. normal/quotient) constraints. Let's now see what constraints the group axioms themselves impose when they interact with the normal/quotient machinery. We already have an identity element (e,e), and we'll see that the inverse-related axioms don't actually impose any constraints beyond those already imposed by associativity. There are two of the latter that any multiplication on G must satisfy, and we'll see that they not only are necessary but also sufficient.

- We defined ν to measure the deviation of u from being a homomorphism. Our first constraint derives from the interaction of ν with associativity.

- **Prop 9.12:** (**Constraint 1**): Given a section u and any multiplication on G adhering to our construction so far, we have $\eta_k(\nu(k',k'')) \cdot \nu(k,k'k'') = \nu(k,k')\nu(kk',k'')$ for some choice of ν.

  Pf: The left side is $\eta_k(\nu(k',k'')) \cdot \nu(k,k'k'') = u(k)\nu(k',k'')u(k)^{-1}\nu(k,k'k'')$, which expands to $u(k)u(k')u(k'')u(k'k'')^{-1}u(k)^{-1}u(k)u(k'k'')u(kk'k'')^{-1} = u(k)u(k')u(k'')u(kk'k'')^{-1}$. The right side is $\nu(k,k')\nu(kk',k'') = u(k)u(k')u(kk')^{-1}u(kk')u(k'')u(kk'k'')^{-1} = u(k)u(k')u(k'')u(kk'k'')^{-1}$, which is the same.

  Note that if our multiplication didn't make (H,e) normal in G or if $K \not\approx G/(H,e)$, we wouldn't be able to define a section u (it would have no meaning). In that case, not only the proof but the premise itself would be ill-defined.

- We also saw that η deviates from being a homomorphism because u does. This deviation also is determined by ν, as the following proposition dictates.

- **Prop 9.13:** (**Constraint 2**): Given a multiplication on G adhering to our construction so far, we have $\eta_k \circ \eta_{k'} = \phi_{\nu(k,k')} \circ \eta_{kk'}$ (where actually $\phi_{\nu(k,k')} \in Inn(N)$, not just $Aut(N)$).

  I.e., the deviation from homomorphism is just $\phi_{\nu(k,k')}(h) = \nu(k,k') \cdot h \cdot \nu(k,k')^{-1}$. As elsewhere, we treat this as taking place in either H or (H,e) as needed.

  Pf: $\eta_k(\eta_{k'}(h,e)) = u(k) \cdot u(k') \cdot (h,e) \cdot u(k')^{-1} \cdot u(k)^{-1}$. On the other hand, $\phi_{\nu(k,k')}(\eta_{kk'}(h,e)) = \nu(k,k') \cdot \eta_{kk'}(h,e) \cdot \nu(k,k')^{-1} = u(k)u(k')u(kk')^{-1}u(kk')(h,e)u(kk')^{-1}u(kk')u(k')^{-1}u(k)^{-1} = u(k)u(k')(h,e)u(k')^{-1}u(k)^{-1}$, which is the same.

  Sometimes people write things like ${}^{k}({}^{k'}h) = {}^{\nu(k,k')}({}^{kk'}h)$. This technically is incorrect because $\nu(k,k') \notin K$. What they really mean is $\phi_{\nu(k,k')}$. The Encyclopedia of Math entry for "group extension" suffers this abuse of notation.

- Why did we label these "constraint 1" and "constraint 2" when they follow from associativity? As mentioned, they also depend on the premise that $(H,e) \triangleleft G$ and $K \approx G/(H,e)$. I.e., any suitable multiplication must satisfy them. They follow from associativity *plus* the normal/quotient premise. As we will see, if we start with an abstract ν and η which satisfy these two constraints, we can construct a multiplication on G which satisfies $(H,e) \triangleleft G$ and $K \approx G/(H,e)$. I.e., these two properties will prove sufficient to create a suitable multiplication.

They also depend on our specific labeling choices via the homomorphisms i and γ (via α). However, as mentioned, we lose no generality in this regard. A different choice of α gives us an SES-isomorphic result, and a different labeling relative to our α just produces a messier expression of the same constraints.

- What about the group inverse axioms? Are there any consequences analogous to those of associativity? It turns out there are no new constraints.

  Pf: Denote by $\delta(k)$ the deviation of u from homomorphism. I.e. $u(k)^{-1} = \delta(k)u(k^{-1})$. Consider $u(k)^{-1}u(k) = e$. This is $\delta(k)u(k^{-1})u(k) = e$. The left side is $\delta(k)\nu(k^{-1},k)u(kk^{-1}) = \delta(k)\nu(k^{-1},k)$ (since we posited $u(e) = (e,e)$). Our constraint is $\delta(k)\nu(k^{-1},k) = e$, which gives us $\delta(k) = \nu(k^{-1},k)^{-1}$. Any ν gives rise to a suitable δ without any further constraint.

We currently are bound to a specific section u. Our η is built from it, and our ν derives from it. What happens if we pick a different section u'?

- When dealing with two sections u and u', we'll denote $\zeta(k) \equiv u'(k)u(k)^{-1}$ and $\overline{\zeta(k)} = u(k)^{-1}u'(k)$. It follows that $\zeta(k)^{-1} = u(k)u'(k)^{-1}$ and $\overline{\zeta(k)}^{-1} = u'(k)^{-1}u(k)$.

  Bear in mind that $u(k)^{-1}$ and $u'(k)^{-1}$ are of the form $(something, k^{-1})$ — though they need not equal $u(k^{-1})$ and $u'(k^{-1})$ — so $\zeta(k)$ and $\overline{\zeta(k)}$ (and, obviously, their inverses) are in (H,e).

- **Prop 9.14:** Suppose we have a multiplication on G. If for some section u with $u(e) = (e,e)$ there exists a ν which (along with the η for that δ) satisfies constraints 1 and 2 above, then for every section u' with $u'(e) = (e,e)$, there exists a corresponding ν' which does so too (with the corresponding η' for that u', of course).

  - Pf: (Part 1: derivation of η'): Let η be for u and η' be for u'. I.e. $\eta_k(h) = u(k)(h,e)u(k)^{-1}$ and $\eta'_k(h) = u'(k)(h,e)u'(k)^{-1}$. Let ν satisfy the two constraints when coupled with u and η. I.e. $\eta_k(\nu(k',k'')) \cdot \nu(k,k'k'') = \nu(k,k')\nu(kk',k'')$ and $\eta_k \circ \eta_{k'} = \phi_{\nu(k,k')} \circ \eta_{kk'}$. Clearly, $\eta'_k(h) = \zeta(k) \cdot \eta_k(h) \cdot \zeta(k)^{-1}$.
  - Pf: (Part 2: derivation of ν'): $\nu'(k,k') = u'(k)u'(k')u'(kk')^{-1}$. But $u'(kk') = \zeta(kk')u(kk') = \zeta(kk')\nu(k,k')^{-1}u(k)u(k')$, so $\nu'(k,k') = \zeta(k)u(k)\zeta(k')u(k')u(k')^{-1}u(k)^{-1}\nu(k,k')\zeta(kk')^{-1}$. This reduces to $\zeta(k)u(k)\zeta(k')u(k)^{-1}\nu(k,k')\zeta(kk')^{-1}$. But $\zeta(k') \in (H,e)$, so we can write $u(k)\zeta(k')u(k)^{-1}$ as $\eta_k(\zeta(k'))$. We thus get $\nu'(k,k') = \zeta(k)\eta_k(\zeta(k'))\nu(k,k')\zeta(kk')^{-1}$.
  - **Cor**: The explicit forms of are:
    * $\eta'_k(h) = \zeta(k) \cdot \eta_k(h) \cdot \zeta(k)^{-1}$
    * $\nu'(k,k') = \zeta(k) \cdot \eta_k(\zeta(k')) \cdot \nu(k,k') \cdot \zeta(kk')^{-1}$
  - **Cor**: We can invert these to get
    * $\eta_k(h) = \zeta(k)^{-1} \cdot \eta'_k(h) \cdot \zeta(k)$
    * $\nu(k,k') = \zeta(k)^{-1} \cdot \eta'_k(\zeta(k'))^{-1} \cdot \nu'(k,k') \cdot \zeta(kk')$

    Pf: The first is trivial. $\nu(k,k') = \eta_k(\zeta(k'))^{-1} \cdot \zeta(k)^{-1} \cdot \nu'(k,k') \cdot \zeta(kk') = \zeta(k)^{-1} \cdot \eta'_k(\zeta(k'))^{-1} \cdot \zeta(k) \cdot \zeta(k)^{-1} \cdot \nu'(k,k') \cdot \zeta(kk')$, which reduces to the result.
  - **Cor**: Some useful forms:
    * ${\eta_k}^{-1}(h) = u(k)^{-1}(h,e)u(k)$.
    * ${\eta_k}^{-1}(h) = \overline{\zeta(k)} \cdot {\eta'_k}^{-1}(h)\overline{\zeta(k)}^{-1}$.

      I.e. ${\eta_k}^{-1}(h) = u(k)^{-1} \cdot u'(k) \cdot {\eta'_k}^{-1}(h) \cdot u'(k)^{-1} \cdot u(k)$
    * ${\eta'_k}^{-1}(h) = \overline{\zeta(k)}^{-1} \cdot {\eta_k}^{-1}(h) \cdot \overline{\zeta(k)}$.

      I.e. ${\eta'_k}^{-1}(h) = u'(k)^{-1} \cdot u(k) \cdot {\eta_k}^{-1}(h) \cdot u(k)^{-1} \cdot u'(k)$

      Note that ${\eta_k}^{-1}$ and ${\eta'_k}^{-1}$ denote inverse automorphisms, while $\zeta(k)^{-1}$ and $\overline{\zeta(k)}^{-1}$ are multiplicative inverses.

      Pf: ${\eta_k}^{-1}(\eta_k(h)) = u(k)^{-1}u(k)(h,e)u(k)^{-1}u(k) = (h,e)$. The other results then follow trivially.

Pf: (Satisfaction of Constraint 1): We need to show that $\eta'_k(\nu'(k',k'')) \cdot \nu'(k,k'k'') = \nu'(k,k') \cdot \nu'(kk',k'')$. The left side expands to $\zeta(k) \cdot \eta_k[\zeta(k') \cdot \eta_{k'}(\zeta(k'')) \cdot \nu(k',k'') \cdot \zeta(k'k'')^{-1}] \cdot \zeta(k)^{-1} \cdot \zeta(k) \cdot \eta_k(\zeta(k'k'')) \cdot \nu(k,k'k'') \cdot \zeta(kk'k'')^{-1}$. The $\zeta(k)^{-1} \cdot \zeta(k)$ cancel and we then can combine the η_k expressions to get $\zeta(k) \cdot \eta_k[\zeta(k') \cdot \eta_{k'}(\zeta(k'')) \cdot \nu(k',k'') \cdot \zeta(k'k'')^{-1} \cdot \zeta(k'k'')] \cdot \nu(k,k'k'') \cdot \zeta(kk'k'')^{-1}$, but this then further reduces to $\zeta(k) \cdot \eta_k[\zeta(k') \cdot \eta_{k'}(\zeta(k'')) \cdot \nu(k',k'')] \cdot \nu(k,k'k'') \cdot \zeta(kk'k'')^{-1}$, which can be rewritten as $\zeta(k) \cdot \eta_k(\zeta(k')) \cdot \eta_k(\eta_{k'}(\zeta(k''))) \cdot \eta_k(\nu(k',k'')) \cdot \nu(k,k'k'') \cdot \zeta(kk'k'')^{-1}$. Since η and ν obey the constraints, we can (constraint 1) replace $\eta_k(\eta_{k'}(\zeta(k'')))$ with $\phi_{nu(k,k')}(\eta_{kk'}(\zeta(k''))) = \nu(k,k')\eta_{kk'}(\zeta(k'')) \cdot \nu(k,k')^{-1}$ and (constraint 2) replace $\eta_k(\nu(k',k'')) \cdot \nu(k,k'k'')$ with $\nu(k,k') \cdot \nu(kk',k'')$. Plugging this all in, we get $\zeta(k) \cdot \eta_k(\zeta(k')) \cdot \nu(k,k') \cdot \eta_{kk'}(\zeta(k''))\nu(k,k')^{-1} \cdot \nu(k,k') \cdot \nu(kk',k'') \cdot \zeta(kk'k'')^{-1}$, which immediately reduces to $\zeta(k) \cdot \eta_k(\zeta(k')) \cdot \nu(k,k') \cdot \eta_{kk'}(\zeta(k'')) \cdot \nu(kk',k'') \cdot \zeta(kk'k'')^{-1}$. Now, let's consider the right side of our original tentative equality. $\nu'(k,k') \cdot \nu'(kk',k'') = \zeta(k) \cdot \eta_k(\zeta(k')) \cdot \nu(k,k') \cdot \zeta(kk')^{-1} \cdot \zeta(kk') \cdot \eta_{kk'} \cdot (\zeta(k''))\nu(kk',k'') \cdot \zeta(kk'k'')^{-1}$, which immediately reduces to $\zeta(k) \cdot \eta_k(\zeta(k')) \cdot \nu(k,k') \cdot \eta_{kk'} \cdot (\zeta(k''))\nu(kk',k'') \cdot \zeta(kk'k'')^{-1}$, which is the same as our reduced expression for the left side.

–

Pf: (Satisfaction of Constraint 2): We need to show that $\eta'_k \circ \eta'_{k'} = \phi_{\nu'(k,k')} \circ \eta'_{kk'}$. First, consider the left side. $\eta'_k(\eta'_{k'}(h)) = \zeta(k) \cdot \eta_k[\zeta(k') \cdot \eta_{k'}(h) \cdot \zeta(k')^{-1}] \cdot \zeta(k)^{-1}$, which we may write as $\zeta(k) \cdot \eta_k(\zeta(k')) \cdot \eta_k(\eta_{k'}(h)) \cdot \eta_k(\zeta(k')^{-1}) \cdot \zeta(k)^{-1}$. But η and nu obey the constraints, so (constraint 1) $\eta_k(\eta_{k'}(h)) = \phi_{\nu(k,k')}(\eta_{kk'}(h)) = \nu(k,k') \cdot \eta_{kk'}(h) \cdot \nu(k,k')^{-1}$, the latter by the definition of ϕ. Substituting this in, we get $\zeta(k) \cdot \eta_k(\zeta(k')) \cdot \nu(k,k') \cdot \eta_{kk'}(h) \cdot \nu(k,k')^{-1} \cdot \eta_k(\zeta(k')^{-1}) \cdot \zeta(k)^{-1}$. Now consider the right side of our tentative equality. $\phi_{\nu'(k,k')}(\eta'_{kk'}(h)) = \nu'(k,k') \cdot \eta'_{kk'}(h) \cdot \nu'(k,k')^{-1}$ by the definition of ϕ. This expands to $\zeta(k) \cdot \eta_k(\zeta(k')) \cdot \nu(k,k') \cdot \zeta(kk')^{-1} \cdot \zeta(kk') \cdot \eta_{kk'}(h) \cdot \zeta(kk')^{-1} \cdot \zeta(kk') \cdot \nu(k,k')^{-1} \cdot \eta_k(\zeta(k'))^{-1} \cdot \zeta(k)^{-1}$, which immediately reduces to $\zeta(k) \cdot \eta_k(\zeta(k')) \cdot \nu(k,k') \cdot \eta_{kk'}(h) \cdot \nu(k,k')^{-1} \cdot \eta_k(\zeta(k'))^{-1} \cdot \zeta(k)^{-1}$. This is the same as our reduced left side.

–

We proved what we called Constraints 1 and 2 above for any multiplication on G for which $(H,e) \triangleleft G$ and $K \approx G/(H,e)$. I.e. they are necessary conditions. Given such a multiplication and any section u for which $u(e) = (e,e)$, we have an η and ν which satisfy them. Let's now show that they are sufficient conditions as well.

- **Prop 9.15:** Given groups H and K and maps $\nu : K \times K \to H$ and $\eta : K \to Aut(H)$ s.t. (a) $\eta(e) = Id_H$, (b) $\nu(k,e) = e$ and $\nu(e,k) = e$ for all $k \in K$, (c) $\eta_k(\nu(k',k'')) \cdot \nu(k,k'k'') = \nu(k,k')\nu(kk',k'')$ for all $k,k',k'' \in K$, and (d) $\eta_k(\eta_{k'}(h)) = \nu(k,k') \cdot \eta_{kk'}(h) \cdot \nu(k,k')^{-1}$ for all $k,k' \in K$ and $h \in H$, there is a group extension (i.e. a multiplication s.t. H is isomorphic to some $N \triangleleft G$ and $K \approx G/N$). Specifically, there is a a group G with elements labeled as (h,k) s.t.
  - (e,e) is the identity.
  - $(h,k)(h',k') = (h \cdot \eta_k(h') \cdot \nu(k,k'), k \cdot k')$ is the multiplication.

    The expression $h \cdot \eta_k(h') \cdot \nu(k,k')$ just involves multiplication on H, since h, $\eta_k(h')$, and $\nu(k,k')$ all are elements of H.
  - $(h,k)^{-1} = (\eta_k{}^{-1}(h^{-1} \cdot \nu(k,k^{-1})^{-1}), k^{-1})$ is the inverse (where $\eta_k{}^{-1}$ is the inverse of the automorphism η_k).

    This also can be written $(\eta_k{}^{-1}(\nu(k,k^{-1}) \cdot h)^{-1}, k^{-1})$.

    Also note that because $\eta : K \to Aut(H)$ is not a homomorphism, $\eta_k^{-1} \neq \eta_{k^{-1}}$. Also, $\eta_k{}^{-1}(h) \neq \eta_k(h)^{-1}$ in general (i.e. the inverse map is not the multiplicative inverse).
  - $i(h) = (h,e)$ is an isomorphism $H \to (H,e)$.
  - $(H,e) \triangleleft G$.
  - $\gamma(h,k) = k$ is a surjective homomorphism $G \to K$ s.t. ker $\gamma = (H,e)$.
  - $K \approx G/(H,e)$.
  - The section $u(k) \equiv (e,k)$ has the provided fns η and ν as its η and ν from our construction.

    I.e., $u(k)u(k')u(kk')^{-1} = \nu(k,k')$ and $u(k)(h,e)u(k)^{-1} = \eta_k(h)$. Note that earlier we started with a multiplication and a u and derived η and ν. Here, we're given η and ν and are constructing a multiplication for which the given section has the specified η and ν as its fns.

    Our multiplication is purely expressed in terms of an abstract η and ν without any reference to a cross-section. How can this be? We have to be careful exactly what is being said here. The multiplication on G is the multiplication on G, regardless of the means by which we initially specified it. This multiplication is expressed in terms of these two functions, nothing more. It is perhaps clearer if we call them foo and bar rather than η and ν. We then can ask whether there is a section u s.t. the associated η is foo and the associated ν is bar. I.e., is there a section which happens to have the specified fns as its ν and η under the specified multiplication.

- This is a lot to unpack, but several of the consequences follow directly from others. For example, the SES involving i and γ is equivalent to the normal/quotient relationship.

- Ok, now for the proofs.
  - First, let's show that the multiplication is associative.

    Pf: associativity): Consider $(h,k)((h',k')(h'',k'')) = (h,k)(h' \cdot \eta_{k'}(h'') \cdot \nu(k',k''), k'k'') = (h \cdot \eta_k(h' \cdot \eta_{k'}(h'') \cdot \nu(k',k'')) \cdot \nu(k,k'k''), kk'k'')$. On the other hand, $((h,k)(h',k'))(h'',k'') = (h \cdot \eta_k(h') \cdot \nu(k,k'), kk')(h'',k'') = (h \cdot \eta_k(h') \cdot \nu(k,k') \cdot \eta_{kk'}(h'') \cdot \nu(kk',k''), kk'k'')$. The 2nd components are equal, so we just need to consider the first and show that $h \cdot \eta_k(h' \cdot \eta_{k'}(h'') \cdot \nu(k',k'')) \cdot \nu(k,k'k'') \overset{?}{=} h \cdot \eta_k(h') \cdot \nu(k,k') \cdot \eta_{kk'}(h'') \cdot \nu(kk',k'')$, which can be rewritten $h \cdot \eta_k(h') \cdot \eta_k(\eta_{k'}(h'')) \cdot \eta_k(\nu(k',k'')) \cdot \nu(k,k'k'') \overset{?}{=} h \cdot \eta_k(h') \cdot \nu(k,k') \cdot \eta_{kk'}(h'') \cdot \nu(kk',k'')$. Removing the identical first factors, we need to show that $\eta_k(\eta_{k'}(h'')) \cdot \eta_k(\nu(k',k'')) \cdot \nu(k,k'k'') \overset{?}{=} \nu(k,k') \cdot \eta_{kk'}(h'') \cdot \nu(kk',k'')$. Applying the 2nd constraint, the left side becomes $\nu(k,k') \cdot \eta_{kk'}(h'') \cdot \nu(k,k')^{-1} \cdot \eta_k(\nu(k',k'')) \cdot \nu(k,k'k'')$. Applying the 1st constraint, it becomes $\nu(k,k') \cdot \eta_{kk'}(h'') \cdot \nu(k,k')^{-1} \cdot \nu(k,k') \cdot \nu(kk',k'')$ which reduces to $\nu(k,k') \cdot \eta_{kk'}(h'') \cdot \nu(kk',k'')$ and equals the right side.

  - (e,e) must be the identity.

    Pf: ((e,e) is the identity): We need to show that $(h,k)(e,e) = (h,k)$ and $(e,e)(h,k) = (h,k)$. $(h,k)(e,e) = (h \cdot \eta_k(e) \cdot \nu(k,e), k \cdot e) = (h,k)$ and $(e,e)(h,k) = (e \cdot \eta_e(k) \cdot \nu(e,k), e \cdot k) = (h,k)$.

  - The inverse can be derived from the multiplication rule.

    Pf: (inverse): Consider the group axiom requirement that $(h,k)(h,k)^{-1} = (e,e)$. Let $(h',k') \equiv (h,k)^{-1}$. Then $(h \cdot \eta_k(h') \cdot \nu(k,k'), kk') = (e,e)$. So, $k' = k^{-1}$ and $h \cdot \eta_k(h') \cdot \nu(k,k') = h \cdot \eta_k(h') \cdot \nu(k,k^{-1})$. I.e., $\eta_k(h') = h^{-1}\nu(k,k^{-1})^{-1}$. η_k is an automorphism, so $h' = {\eta_k}^{-1}(h^{-1}\nu(k,k^{-1})^{-1})$, where ${\eta_k}^{-1}$ is the inverse map and the other inverses are multiplicative inverses. Note that η (as a map $K \to Aut(N)$) is *not* a homomorphism, so we *can't* write the inverse map ${\eta_k}^{-1}$ as $\eta_{k^{-1}}$. We thus must content ourselves with $h' = {\eta_k}^{-1}(h^{-1}\nu(k,k^{-1})^{-1})$.

  - Next, let's prove the core of the theorem: that the multiplication in question produces the desired normal/quotient relation involving H and K.

    Pf: (i is an isomorphism): i trivially is bijective. Let's show that i^{-1} is a homomorphism. A bijective homomorphism is an isomorphism, so it then would follow that i^{-1} (and hence i) is an isomorphism. By definition $i(e) = (e,e)$, which we showed is the identity on G. $(h,e)(h',e) = (h \cdot \eta_e(h')\nu(e,e), e \cdot e) = (hh',e)$ (since $\nu(e,e) = e$). So i^{-1} is a homomorphism and we're done.

    Pf: (γ is a surjective homomorphism): γ trivially is surjective. $\gamma(e,e) = e$. Consider $\gamma((h,k)(h',k')) = \gamma(h\eta_k(h')\nu(k,k'), kk') = kk'$. So γ is a homomorphism.

    Pf: ($\ker \gamma = (H,e)$): $\ker \gamma = \gamma^{-1}(e)$, but $\gamma(h,k) = k$, so $\gamma^{-1}(e) = (H,e)$.

    Pf: ($(H,e) \triangleleft G$): This follows because $(H,e) = \ker \gamma$ and γ is a surjective homomorphism. By the First Homomorphism Thm, (H,e) is normal in G.

    Pf: ($K \approx G/(H,e)$): Again, by the First Homomorphism Thm, since we have a surjective homomorphism γ, $K \approx G/\ker \gamma = G/(H,e)$.

  - Finally, we'll show that the specified u has the correct η and ν.

    Pf: (Proof for η): $(e,k) \cdot (h,e) \cdot (e,k)^{-1} = (e\eta_k(h)\nu(k,e), k) \cdot ({\eta_k}^{-1}(e\nu(k,k^{-1})^{-1}), k^{-1})$. The 2nd component is e and the first reduces to $\eta_k(h) \cdot \eta_k({\eta_k}^{-1}(\nu(k,k^{-1})^{-1}))\nu(k,k^{-1})$. But $\eta_k \circ {\eta_k}^{-1} = Id_H$, so we get $\eta_k(h) \cdot \nu(k,k^{-1})^{-1} \cdot \nu(k,k^{-1}) = \eta_k(h)$.

    Pf: (proof for ν): $(e,k)(e,k') = (e\eta_k(e)\nu(k,k'), kk') = (\nu(k,k'), kk')$. On the other hand, $(\nu(k,k'), e)(e, kk') = (\nu(k,k')\eta_e(e)\nu(e,k), kk') = (\nu(k,k'), kk')$. So $u(k)u(k') = \nu(k,k')u(kk')$.

    I.e., given our 2 fns, we can define a multiplication on G of the form specified. Under this multiplication, the section $u(k) \equiv (e,k)$ has the 2 fns as its η and ν. Given any other section u', this same multiplication looks different in terms of the corresponding η' and ν' for u' — but is the same multiplication (we'll exhibit it momentarily). On the other hand, if we were given *that* η' and ν' then a different multiplication on G has those as the η and ν for the (e,k) section.

- Suppose we pick some other section u'. It has its own associated η' and ν', given by $\eta'_k(h) = u'(k)(h,e)u'(k)^{-1}$ and $\nu'(k,k') = u'(k)u'(k')u'(kk')^{-1}$. We can do two things with these.
  - (i) Use these as the η and ν for a group construction of the form in the theorem. We get a different group G' because its multiplication now is built (using the same formula of the thm) from η' and ν'. Obviously, talking of u' is meaningless relative to G'. Though the labels still exist (since set-wise we're labeling points in $H \times K$ in both G and G'), the section u' has no special place in G'. The section with this μ' and ν' as its μ and ν in G' is (e,k), just as the multiplication formula is the usual one but now with η' and ν' in place of the old η and ν. I.e., the only role of u' in this approach is to obtain

η' and ν', which we then use to build a new group. As we will see, any such G' is SES-equivalent to G.

- (ii) We can express the multiplication on G in terms of η' and ν'. The multiplication is unchanged, but its expression in terms of η' and ν' is different from its expression in terms of η and ν. Let's now see how they are related.

To use a basis change analogy from linear algebra, loosely speaking one of these corresponds to a change of basis while the other corresponds to an active transformation.

- **Prop 9.16:** Given the setup of the theorem and a different section u' with corresponding η' and ν', the multiplication and inverse in terms of this η' and ν' are given by:
  - $(h,k)\cdot(h',k') = (h\cdot\zeta(k)^{-1}\cdot\eta'_k(h'\zeta(k')^{-1})\cdot\nu'(k,k')\cdot\zeta(kk'),kk')$.
  - $(h,k)^{-1} = ({\eta'_k}^{-1}((h\zeta(k)^{-1})^{-1}\nu'(k,k^{-1})^{-1})\cdot\zeta(k^{-1}),k^{-1})$.

I.e., we don't just replace η with η' and ν with ν', but effectively replace (h,k) with $(h\zeta(k)^{-1},k)$. What about the factors of $\zeta(kk')$ and $\zeta(k^{-1})$ at the end of the two expressions? That too is a result of replacing (h,k) with $(h\zeta(k)^{-1},k)$. We convert our pts from (h,k) to $(h\zeta(k)^{-1},k)$, etc. Then we apply the usual expressions, as if η' and ν' were our fns. The result is of the form $(\tilde{h},\tilde{k})$, but this is transformed. To get back to the true answer (h_{true},k_{true}) we must reverse the mapping, so $k_{true}=\tilde{k}$ and $h_{true}\zeta(\tilde{k})^{-1}=\tilde{h}$. I.e. $h_{true}=\tilde{h}\cdot\zeta(\tilde{k})$. In the case of multiplication, $\tilde{k}=kk'$ and in the case of the inverse $\tilde{k}=k^{-1}$. Put another way, the usual multiplication and inverse expressions hold for η' and ν' but in the rotated space $(h\zeta(k)^{-1},k)$. This also gives us some insight into the type of alternate multiplication we get if we truly use η' and ν' as our input fns. In that case, we get the same multiplication but operating on pts in the transformed G given by $(h,k)\rightarrow(h\zeta(k)^{-1},k)$. This is no surprise, because we're simply replacing u by u' as our reference section so it makes sense the effect would be to rotate the H part of $H\times K$ in the opposite direction by $u(k)u'(k)^{-1}$.

Pf: (multiplication): For multiplication, the 2nd term still is kk'. The first term is $h\eta_k(h')\nu(k,k') = h\zeta(k)^{-1}\eta'_k(h')\zeta(k)\zeta(k)^{-1}\eta'_k(\zeta(k'))^{-1}\nu'(k,k')\zeta(kk') = h\zeta(k)^{-1}\eta'_k(h')\eta'_k(\zeta(k'))^{-1}\nu'(k,k')\zeta(kk')$. Since η_k is a homomorphism, this is just $h\zeta(k)^{-1}\eta'_k(h'\cdot\zeta(k')^{-1})\nu'(k,k')\zeta(kk')$, the form stated.

Pf: (inverse): For the inverse, the 2nd term still is k^{-1}. The 1st term is ${\eta_k}^{-1}(h^{-1}\nu(k,k^{-1})^{-1})$. Fully expanded in terms of u, this is $u(k)^{-1}h^{-1}u(k\cdot k^{-1})^{-1}u(k^{-1})^{-1}u(k)^{-1}u(k)$. Noting that $u(e)=e$ and reducing the expression we have $u(k)h^{-1}u(k^{-1})^{-1}$. Since u is not a homomorphism, further reduction is not possible. Now consider the expression ${\eta'_k}^{-1}((h\zeta(k)^{-1})^{-1}\nu'(k,k^{-1})^{-1})\cdot\zeta(k^{-1})$. Expanding in terms of u' and u, we have $u'(k)^{-1}u'(k)u(k)^{-1}h^{-1}u'(k\cdot k^{-1})^{-1}u'(k^{-1})^{-1}u'(k)^{-1}u'(k)u'(k^{-1})u(k^{-1})^{-1}$. This immediately reduces to $u(k)^{-1}h^{-1}u(k^{-1})^{-1}$, which is the same.

- **Prop 9.17:** Let G be constructed via our programme from groups H and K and a suitable η and ν, and let G' be constructed via our programme from groups H and K and a suitable η' and ν', and let η' and ν' are relate to η and ν by the section-change rule above (i.e., η' and ν' are the relevant η and ν for some other section of G, which need not be the case in general). Then not only does $G\approx G'$, but the group extensions are SES-equivalent.

I.e., for a given H and K, the group extensions are partitioned into equivalence classes by the section-change relationship. Note that these need not equal the SES-equivalence classes per-se because the there also may be SEs-equivalences which are not related in this way. I.e., the partition thus engendered can be a refinement of SES-equivalence. Put another way, multiple of our equivalence classes may form each SES-equivalence class.

Pf: Suppose we are given such a G (built from η and ν) and G' (built from η' and ν'), and that u is the usual section of G (i.e. (e,k)) and u' is the section of G with η' and ν' as its fns. As usual, we'll denote $\zeta(k)\equiv u'(k)u(k)^{-1}$ (in G). Define the map $\gamma : G\rightarrow G'$ via $\gamma(h,k)\equiv(h\zeta(k)^{-1},k)$. Clearly, γ is bijective and slice-preserving since all it does it translate the elements of slice k by $\zeta(k)^{-1}$. Since $u(e)=u'(e)=e$, $\zeta(e)=e$ and $\gamma(e,e)=(e,e)$. As for multiplication, $\gamma(h,k)=(h\zeta(k)^{-1},k)$ and $\gamma(h',k')=(h'\zeta(k)^{-1},k)$, so $\gamma(h,k)\gamma(h',k')=(h\cdot\zeta(k)^{-1}\cdot\eta'_k(h'\zeta(k)^{-1})\cdot\nu'(k,k'),kk')$. On the other hand, $\gamma((h,k)(h',k'))=\gamma(h\cdot\eta_k(h')\cdot\nu(k,k'),kk')=(h\cdot\eta_k(h')\cdot\nu(k,k')\cdot\zeta(kk')^{-1},kk')$. The second components match up, but what about the first? Since η and ν are related to η' and ν' via a section-change, we have the relationship above and $h\cdot\eta_k(h')\cdot\nu(k,k')=h\cdot\zeta(k)^{-1}\cdot\eta'_k(h'\zeta(k')^{-1})\cdot\nu'(k,k')\cdot\zeta(kk')$. This can be rephrased as $h\cdot\eta_k(h')\nu(k,k')\zeta(kk')^{-1}=h\cdot\zeta(k)^{-1}\cdot\eta'_k(h'\zeta(k')^{-1})\cdot\nu'(k,k')$, and the first components are equal. γ is a bijective homomorphism and thus an isomorphism, so $G\approx G'$. To see SES-equivalence, we first note that γ restricts to an isomorphism between $(H,e)\subset G$ and $(H,e)\subset G'$. In fact, it induces the identity automorphism on H. The restriction is $\gamma(h,e)=(h,e)$ since $\gamma(e)=e$. Since the group multiplication is the same (via isomorphism) and the normal subgroup is the same, so is the quotient group. K labels it the same way, since G and G' only differ in their behavior within slices. Formally, the SES for G is $e\rightarrow H\xrightarrow{i}G\xrightarrow{q}K\rightarrow e$ and for G' it is $e\rightarrow H\xrightarrow{i}G'\xrightarrow{q}K\rightarrow e$, with the same i and q. How can this be? γ effectively is an automorphism of G. It has no effect on $(H,e)\subset G$ and has no effect on $G/(H,e)$. All it does is relabel elements (slightly) within each $k\neq e$ slice. We thus have an SES-equivalence.