Group Theory 3
Semi-direct products, nilpotent groups, and solvable groups
by Ivan Aidun

These are notes interspersed with exercises. The purpose of these notes is to be more fleshed out than Evan Dummit's old notes, but shorter and more focused than a textbook treatment. Halfway between Dummit and Dummit and Foote, so to speak. I hope these are helpful to you!

Semidirect products

An example

I'm going to begin describing semidirect products with an example you already know, dressed up in an unfamiliar garment. Often, we think about the group $\mathbb{Z}/n\mathbb{Z}$ acting on an n-gon by rotations. Imagine an n-gon made out of one continuous pipe, and within the pipe there is a fluid flowing around (maybe it's some modern art piece which nobody understands). Consider the group which acts on this object, where the possible symmetries are to rotate the n-gon *in the direction of the fluid flow*, or to reverse the direction the fluid is flowing.

We will call this group the *oriented cyclic group of order* n, OC_n, and concretely the elements of this group are pairs of the form (a, o), where $a \in \mathbb{Z}/n\mathbb{Z}$ is the *position* of the element (how much we're rotating), and $o \in \{\pm 1\}$ is the *orientation* (whether or not we're reversing the flow after the rotation). The group multiplication is defined so that the orientations multiply, so the composition of two negatively oriented elements is positively oriented. The positions add normally if they are both positively oriented, but if the first element is negatively oriented, instead the second position is subtracted from the first, because in that case the second rotation will happen in the opposite direction. In symbols, in all cases we have:

$$(a_1, o_1) \cdot (a_2, o_2) = (a_1 + o_1 a_2, o_1 o_2).$$

For example, if $n = 5$, here are a few computations in this group:

$$(3,1)\cdot(2,-1) = (0,-1), \qquad (1,-1)\cdot(3,-1) = (1,1),$$
$$(2,-1)\cdot(3,1) = (4,-1), \qquad (3,-1)\cdot(1,-1) = (2,1).$$

Exercise 1.

(a) Verify that OC_n is a group. Is the multiplication associative? What is the identity? What is the inverse of (a, o)?

(b) What is the order of OC_n?

(c) Write out the multiplication table for OC_3. Yes, I'm serious.

(d) What is the more common name for this family of groups?

I have disguised these groups you already know in order to emphasize somewhat that this construction depended only on one thing: the fact that the groups $\mathbb{Z}/n\mathbb{Z}$ all have an action by a cyclic group of order 2, namely $a \mapsto -a$. This isn't just an action of $\{\pm 1\}$ on a *set* of size n that coincidentally happens to be a group: in addition, the map $a \mapsto -a$ is a group homomorphism $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Inside the group OC_n (I'm not dropping the pretense), we can see how to get $-a$: first reverse the fluid flow, then rotate by a, then reverse the fluid flow back. In symbols: $(-a, 1) = (0, -1) \cdot (a, 1) \cdot (0, -1)^{-1}$. The negation action is built into the group as a conjugation!

The general case

Let N, Q be groups such that Q acts on N on the left. As mentioned, we are going to require that the action of Q on N "respects the group structure", so instead of Q acting on N by arbitrary functions, we want for Q to act on N by homomorphisms. This means that the action satisfies $(q \cdot n_1)(q \cdot n_2) = q \cdot (n_1 n_2)$, where $q \cdot n$ indicates the action of q on the element n. If we think about a general group action as a homomorphism $Q \to S_N$, here instead I'm asking for a homomorphsim $Q \to \mathrm{Aut}(N)$.

If we have such an action, we can construct the **semidirect product** $N \rtimes Q$. The semidirect product is a group whose underlying set is $N \times Q$, with multiplication defined by $(n_1, q_1)(n_2, q_2) = (n_1(q_1 \cdot n_2), q_1 q_2)$. You should think of this as *almost* being the direct product $N \times Q$, but the multiplication law has been "twisted" by the action of Q. It might be better to call this *one* semi-direct product of N and Q, because we can get non-isomorphic products by choosing different actions of Q on N (always satisfying $(q \cdot n_1)(q \cdot n_2) = q \cdot (n_1 n_2)$).

With this definition, one can see that $N \rtimes Q$ has a normal subgroup isomorphic to N consisting of elements of the form (n, e_Q), and a subgroup isomorphic to Q consisting of elements of the form (e_N, q). The explanation for the cryptic multiplication is that it is defined so that conjugating an element of the normal subgroup (n, e_Q) by (e_N, q) corresponds to the action of q on n: $(e_N, q)(n, e_Q)(e_N, q^{-1}) = (q \cdot n, e_Q)$. Thus, our original group action has been "encoded" in the semidirect product as an action by conjugation. The subgroup isomorphic to Q need not be normal, as fixing an element $n \in N$, the set of elements $\{(n(q \cdot n^{-1}), q) : q \in Q\}$ forms a conjugate subgroup.

As noted above, which specific action you choose of Q on N can change the isomorphism type of the group $N \rtimes Q$. In situations where more than one semidirect product between the same two groups might come up, people will name the actions, e.g. $\phi, \psi \colon Q \to \mathrm{Aut}(N)$, and write $N \rtimes_\phi Q$ versus $N \rtimes_\psi Q$.

Notice that the direct product is a special case of the semidirect product: if $Q \circlearrowright N$ trivially via $q \cdot n = n$ for all pairs $q \in Q$ and $n \in N$, then $N \rtimes Q = N \times Q$.

Exercise 2. How many nonisomorphic groups of the form $\mathbb{Z}/7\mathbb{Z} \rtimes C_6$ are there?

Semidirect products and splitting sequences

If N, Q are groups, and $Q \circlearrowright N$ by homomorphisms, then there is a SES of groups

$$1 \to N \to N \rtimes Q \to Q \to 1.$$

Moreover, this exact sequence splits on the right, via the map $q \mapsto (e_N, q)$. More generally, whenever $N \triangleright G$, if the exact sequence

$$1 \to N \to G \to G/N \to 1$$

splits on the right, then $(G/N) \circlearrowright N$ via conjugation, and $G \cong N \rtimes G/N$. In this case, letting H be the image of the splitting homomorphism, we say that G is the **internal semidirect product** of N and H.

With groups there is a real difference between a SES splitting on the right versus on the left. If the SES

$$1 \to N \to G \to G/N \to 1$$

splits on the left, then not only is $G \cong N \rtimes G/N$, but actually $G \cong N \times G/N$.

Exercise 3. Consider the group $G = \mathrm{SL}_2(\mathbb{F}_3)$.

(a) What is the order of G?

(b) Show that G has a subgroup H isomorphic to Q.

(c) Show that H is normal.

(d) Prove that $G \cong Q \rtimes C_3$ by finding a splitting map $C_3 \cong G/H \to G$.

The semidirect product test

There's a standard test to show that G is the (internal) semidirect product of its subgroups N and Q. If:

- N is normal in G,
- $N \cap Q = \{e\}$ is the set containing only the identity element, and
- $G = NQ$ (that is, every element $g \in G$ can be written as nq for some $n \in N$ and $q \in Q$)

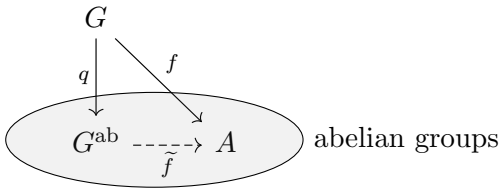
then $G = N \rtimes Q$ (where the action of Q on N is conjugation in G).

The commutator (derived) subgroup

An important subgroup of a group is the commutator subgroup, sometimes also called the derived subgroup. (I will not call it that because I think this terminology is misleading if you're familiar with other uses of the term "derived".) The **commutator subgroup** of G, denoted $[G, G]$, is the group generated by elements of the form $ghg^{-1}h^{-1}$, which are called **commutators**. This means a general element of $[G, G]$ will look like $g_1h_1g_1^{-1}h_1^{-1} \dots g_nh_ng_n^{-1}h_n^{-1}$. You will also (in the next section) see the notation $[H_1, H_2]$ for H_1, H_2 subgroups of a given group G. In this case, the notation means the subgroup generated by commutators $h_1h_2h_1^{-1}h_2^{-1}$ where $h_i \in H_i$, $i = 1, 2$.

The commutator subgroup will be trivial if and only if G is abelian. For any group G, $[G,G]$ is a normal subgroup of G. Here's a tricky way to see this, relying on the fact that commutators and conjugation are closely linked: suppose $x \in [G,G]$, and $g \in G$, then $gxg^{-1}x^{-1} \in [G,G]$ because it is a commutator, so call $y = gxg^{-1}x^{-1}$. Then we have $gxg^{-1} = yx$, and $yx \in [G,G]$ since both of $x, y \in [G,G]$.

Furthermore, $G/[G,G]$ is always an abelian group, since in the quotient every commutator is trivial. The group $G/[G,G]$ is called the *abelianization* of G, denoted G^{ab}. It has the universal property: if A is an abelian group, and $f\colon G \to A$ is a homomorphism, then there exists a unique homomorphism $\widetilde{f}\colon G^{\text{ab}} \to A$ so that $f = \widetilde{f} \circ q$, where $q\colon G \to G^{\text{ab}}$ is the quotient map. In diagram form:



This is akin to the universal property of $S^{-1}M$, and analogous to my comment in that section, you should think of the abelianization as the "best abelian approximation" to G. When G is finite, the universal property has a payout in terms of sizes: G^{ab} is the largest abelian quotient of G.

Exercise 4. For each of the following groups G, compute $[G,G]$.

(a) D_4

(b) Q

(c) S_4

(d) A_4

(e) A_5

Sometimes, a group G might not admit *any* nontrivial maps to an abelian group, which would happen when $G^{\text{ab}} = 1$, or to say it another way, when $[G,G] = G$. Such a group is called **perfect**.

Exercise 5. In this problem we will show that $G = \mathrm{SL}_2(\mathbb{F}_5)$ is a perfect group. Call a matrix $A \in \mathrm{SL}_2(\mathbb{F}_5)$ a *sheering matrix* if A is upper or lower triangular with 1s on the diagonal.

(a) Prove that $\mathrm{SL}_2(\mathbb{F}_5)$ is generated by the two matrices

$$S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

(b) Prove that T can be written as a product of sheering matrices. Conclude that the sheering matrices generate $\mathrm{SL}_2(\mathbb{F}_5)$.

(c) Prove that any two sheering matrices in $\mathrm{SL}_2(\mathbb{F}_5)$ are conjugate to one another. (Hint: try conjugating S by matrices of the form D or TD, where D is diagonal.)

(d) Use your previous computations to prove that S or some other sheering matrix lies in $[G, G]$. Conclude that $[G, G] = G$.

Observe that $\mathrm{SL}_2(\mathbb{F}_5)$ is not simple because it has a nontrivial center. It is the smallest perfect group that is not a simple group. Showing that matrix groups are perfect comes up because Tits' simplicity theorem lets you upgrade a group being perfect (plus some extra stuff) into that group being simple.

Nilpotent groups

A nilpotent group is a generalization of an abelian group. There are two equivalent definitions of nilpotent groups:

- G is nilpotent if the descending sequence of normal subgroups $G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots$ eventually terminates in the trivial subgroup, where $G_{i+1} = [G_i, G]$.
- G is nilpotent if the ascending sequence of normal subgroups $\{e\} = Z_0 \triangleleft Z_1 \triangleleft Z_2 \triangleleft \dots$ eventually terminates in the full group G, where Z_{i+1} is defined so that $Z_{i+1}/Z_i = Z(G/Z_i)$. **Exercise 6.** Confirm that this gives a well-defined subgroup.

These are respectively called the **lower central series** and the **upper central series**. If these series terminate, their lengths are the same, and the length of either series is called the *nilpotency class* of G. The groups of nilpotency class 1 are exactly the abelian groups.

Exercise 7. (What's a central series?) There is a general definition of a "central series", altho I think historically it was invented in retrospect to solidify the things that the lower and upper central series have in common. A **central series** is a sequence of normal subgroups $G = A_0 \triangleright A_1 \triangleright \cdots \triangleright A_n = \{e\}$ that satisfy either of the two conditions

(i) $[G, A_i] < A_{i+1}$, or

(ii) $A_i/A_{i+1} < Z(G/A_{i+1})$.

I will write A^i to mean A_{n-i}.

(a) Prove that conditions (i) and (ii) above are equivalent.

(b) Given any central series A_i, prove that $A_i > G_i$.

(c) Given any central series A^i, prove that $A^{i+1}/A^i < Z(G/Z_i)$.

(d) Conclude that any central series has the same length.

Exercise 8. A finite group is called a **p-group** if $\#G = p^k$ for some k. Fix an arbitrary finite nontrivial p-group G.

(a) Show that $Z(G) \neq \{e\}$.

(b) Show that G is nilpotent.

Why are nilpotent groups called "nilpotent"? There doesn't seem to be anything particularly nilpotent-y about them. The term originally comes from the theory of Lie groups and Lie algebras. Here's one possible way to think about it: for each $g \in G$ we can define a function $f_g \colon G \to G$ by $f_g(x) = [g, x] = gxg^{-1}x^{-1}$. This function is not a homomorphism, it's just a function. A group is called nilpotent if there exists some n such that for all g, f_g^n is the trivial map $G \to \{e\}$, i.e. if each of the functions f_g is "nilpotent" in a more normal sense of the word.

Solvable groups

Another generalization of abelian groups are solvable groups. A group is **solvable** if there exists a sequence of subgroups $G = G_0 > G_1 > \cdots > G_n = \{e\}$ such that (i) $G_{i+1} \triangleleft G_i$ and (ii) the quotients G_i/G_{i+1} are all abelian. The terminology comes from Galois theory, as a polynomial can be solved by radicals if and only if its Galois group is a solvable group.

Given a group, it might be difficult to come up with such a sequence of subgroups just by thinking and messing around. Luckily, there's a standard sequence that you can always check. Given a group G, the **derived series** of G is the sequence of subgroups $G = G^{(0)} > G^{(1)} > G^{(2)} > \dots$ where $G^{(i+1)}$ is the commutator subgroup of the preceding group $[G^{(i)}, G^{(i)}]$. (I would prefer to call this the "commutator series", but it seems like in actual practice nobody does that.)

Exercise 9. The derived series is usually not the same as the lower central series. The difference in the definition is $G^{(i+1)} = [G^{(i)}, G^{(i)}]$ versus $G_{i+1} = [G, G_i]$. Find an example of a group G demonstrating that these two series can be different.

Exercise 10. Prove that a finite group G is solvable if and only if the derived series eventually reaches the trivial group.

Exercise 11.

(a) Prove that any nilpotent group is solvable.

(b) Find an example of a group that is solvable but not nilpotent.

Exercise 12. Let $1 \to A \to B \to C \to 1$ be a short exact sequence of groups. Show that if A and C are solvable, then B is also solvable.

Exercise 13. (August 2019 Problem 5) Let G be the group of 2×2 invertible upper triangular matrices over the field $\mathbb{F}_p$.

(a) Prove that G has only one subgroup of order p, and that this subgroup is normal. (Hint: first show that an element of order p must have 1's on the diagonal.)

(b) Prove that G is solvable by exhibiting a homomorphism f from G to an abelian group A such that the kernel of f is also abelian.

(c) Prove that if $p \neq 2$, G is not nilpotent.

Exercise 14. (January 2022 Problem 1) On this problem, only the answer will be graded. Consider the symmetric group S_4.

(a) What is the order of S_4?

(b) What is the order of its center $Z(S_4)$?

(c) What is the order of its commutator subgroup $[S_4, S_4]$?

(d) Is S_4 a simple group?

(e) Is S_4 a solvable group?

(f) How many conjugacy classes does S_4 have?

Some other problems I like

Exercise 15. The additive group $\mathbb{Q}$ has the property that for any $q \in \mathbb{Q}$ and any $n \in \mathbb{Z}$, there exists an element $q' \in \mathbb{Q}$ such that $nq' = q$ (in particular $q' = q/n$). An abelian group with this property is called a *divisible* group.

(a) Show that any nontrivial divisible group is infinite.

(b) Show that if G is divisible, and N is a subgroup (normal since G is abelian), then G/N is divisible.

Exercise 16. (January 2017 Problem 1, (d) omitted) Give an example of each of the following.

(a) A group G with a normal subgroup N such that G is not a semidirect product $N \rtimes G/N$.

(b) A finite group G that is nilpotent but not abelian.

(c) A group G whose commutator subgroup $[G, G]$ is equal to G.

(e) A transitive action of S_3 on a set X of cardinality greater than 3.