Math 5111 (Algebra 1)

Lecture #17 of 24 $\sim$ November 9th, 2020

Products of Subgroups

- Products of Subgroups
- Semidirect Products

This material represents §3.4.3-3.4.4 from the course notes.

Products of Subgroups, I

We proved earlier that every finitely generated abelian group decomposes as a direct product of cyclic groups.

- This result tells us that finitely generated abelian groups can be built up from subgroups by taking products.
- We can often piece other groups together from subgroups in a similar way.
- We would like to study how to do this, because it will give us more ways to construct finite groups and classify groups of a given order.

Products of Subgroups, II

If H and K are subgroups of G, then we can certainly consider the subgroup $\langle H, K \rangle$ generated by H and K.

- However, the elements in this subgroup are hard to write down in general, since they are words of arbitrary length in the elements of H and K.
- If elements from H and K commute with one another, then by rearranging the elements in the word and using the fact that H and K are closed under multiplication, we can reduce any word to a product of the form hk for $h \in H$ and $k \in K$.
- We will now look at the same set of elements for arbitrary subgroups: this is the idea of the product of two subgroups.

Products of Subgroups, III

Definition

If H and K are subgroups of G, then the <u>product</u> HK is the set $HK = \{hk : h \in H, k \in K\}$.

The product of two subgroups is not necessarily a subgroup of G.

- For example, for $H = \{1, (1\,2)\}$, $K = \{1, (1\,3)\}$ in $G = S_3$, the product $HK = \{1, (1\,2), (1\,3), (1\,3\,2)\}$, which is not a subgroup of G.
- However, in some cases HK will be a subgroup: for example, with $H = \{1, (1\,2)\}$ and $K = \{1, (3\,4)\}$ in $G = S_4$, then $HK = \{1, (1\,2), (3\,4), (1\,2)(3\,4)\}$ is indeed a subgroup of G.

Products of Subgroups, IV

We have various properties of subgroup products:

Proposition (Products of Subgroups)

Let G be a group and H and K be subgroups of G.

1. *If H and K are finite, then $\#(HK) = \dfrac{\#H \cdot \#K}{\#(H \cap K)}$.*
2. *The product HK is a subgroup of G if and only if $HK = KH$.*
3. *If $H \le N_G(K)$ or $K \le N_G(H)$, then HK is a subgroup of G.*
4. *If H or K is normal in G, then HK is a subgroup of G.*
5. *If both H and K are normal in G, and $H \cap K = \{e\}$, then HK is isomorphic to the direct product $H \times K$.*
6. *If $n_p = 1$ for every prime p dividing $\#G$, then G is the (internal) direct product of its Sylow subgroups. Such groups are called nilpotent groups.*

Products of Subgroups, V

Proofs:

1. If H and K are finite, then $\#(HK) = \dfrac{\#H \cdot \#K}{\#(H \cap K)}$.
   - Observe that HK is a union of left cosets of K: specifically: $HK = \cup_{h \in H} hK$.
   - Thus we need only count how many distinct left cosets are obtained, since each left coset has cardinality $\#K$.
   - Consider the action of H by left multiplication on the left cosets of K in HK: by definition, there is a single orbit for this action.

Products of Subgroups, VI

Proofs:

1. If H and K are finite, then $\#(HK) = \dfrac{\#H \cdot \#K}{\#(H \cap K)}$.
   - Notice that the stabilizer of the left coset eK is the set of $h \in H$ with $h \cdot eK = eK$, which is equivalent to saying $h \in K$.
   - Thus, the stabilizer is simply the set of $h \in H$ such that $h \in K$, which is to say, it is the intersection $H \cap K$.
   - So by the orbit-stabilizer theorem, the size of the orbit is equal to the index $[H : H \cap K]$. This means $\#(HK) = \#K \cdot [H : H \cap K] = \dfrac{\#H \cdot \#K}{\#(H \cap K)}$, as claimed.

Remark: If H or K is infinite, then trivially HK is also infinite. We also emphasize that HK is not assumed to be a subgroup here.

Products of Subgroups, VII

Proofs:

2. The product HK is a subgroup of G if and only if $HK = KH$.
   - First suppose $HK = KH$.
   - Let $g = hk$ and $g' = h'k'$ be elements of HK, with $h, h' \in H$ and $k, k' \in K$.
   - Then since $HK = KH$, the element $kh' \in KH$ is of the form $h''k''$ for some $h'' \in H$ and $k'' \in K$.
   - Then $gg' = hkh'k' = h(kh')k' = h(h''k'')k' = (hh'')(k''k') \in HK$.
   - Likewise, $g^{-1} = k^{-1}h^{-1} \in KH = HK$. Since the identity $e = ee$ is clearly in HK, this means HK is a subgroup of G.

Products of Subgroups, VIII

Proofs:

2. The product HK is a subgroup of G if and only if $HK = KH$.
   - Conversely, suppose HK is a subgroup.
   - Then since H and K are both in HK, we have $\langle H, K\rangle = HK$ and so $KH \subseteq \langle H, K\rangle = HK$.
   - For the other containment, suppose $k \in K$ and $h \in H$.
   - Then we have $h^{-1}k^{-1} \in HK$, so since HK is closed under inverses, we see $(h^{-1}k^{-1})^{-1} = kh$ must be in HK for any k, h.
   - Thus, $HK \subseteq KH$, and so in fact $HK = KH$.

Products of Subgroups, IX

Proofs:

3. If $H \leq N_G(K)$ or $K \leq N_G(H)$, then HK is a subgroup of G.
   - Suppose $H \leq N_G(K)$, and let $h \in H$ and $k \in K$.
   - By hypothesis, $hkh^{-1} \in K$, and therefore we can write $hk = (hkh^{-1})h \in KH$.
   - Thus, $hk \in KH$, and so $HK \subseteq KH$.
   - Likewise, $kh = h(h^{-1}kh) \in HK$, and so $KH \subseteq HK$.
   - We therefore have $KH = HK$, and so HK is a subgroup of G by (2).
   - The case where $K \leq N_G(H)$ is essentially identical.

Products of Subgroups, X

Proofs:

4. If H or K is normal in G, then HK is a subgroup of G.
   - If H is normal in G, then $N_G(H) = G$.
   - Thus, trivially $K \leq N_G(H)$. So by (3), HK is a subgroup of G.
   - Likewise, if K is normal in G, then $H \leq G = N_G(K)$, so again by (3), HK is a subgroup of G.

Products of Subgroups, XI

Proofs:

5. If both H and K are normal in G, and $H \cap K = \{e\}$, then HK is isomorphic to the direct product $H \times K$.
   - Since H is a normal subgroup of G, by (4) that means HK is a subgroup of G.
   - We first show that the elements of H commute with the elements of K.
   - To see this, observe that if $h \in H$ and $k \in K$, then $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1}$ is an element of K, since $hkh^{-1} \in K$ since K is normal in G.
   - But $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1})$ is also an element of H, since $kh^{-1}k^{-1} \in H$ since H is normal in G.
   - This means $hkh^{-1}k^{-1} \in H \cap K$, and so $hkh^{-1}k^{-1} = e$, meaning that $hk = kh$: thus, h and k commute.

Products of Subgroups, XII

Proofs:

5. If both H and K are normal in G, and $H \cap K = \{e\}$, then HK is isomorphic to the direct product $H \times K$.
   - Next, we claim that every element of HK can be written uniquely in the form hk with $h \in H$ and $k \in K$.
   - To see this suppose $hk = h'k'$ for $h, h' \in H$ and $k, k' \in K$. Then $(h')^{-1}h = k'k^{-1}$. But the left-hand side is an element of H while the right-hand side is an element of K, so by the assumption $H \cap K = \{e\}$, this common element must be the identity e.
   - Thus $(h')^{-1}h = e = k'k^{-1}$ and so $h' = h$ and $k' = k$, meaning h and k are unique.

Products of Subgroups, XIII

Proofs:

5. If both H and K are normal in G, and $H \cap K = \{e\}$, then HK is isomorphic to the direct product $H \times K$.
   - Therefore, we have a well-defined map $\varphi : HK \to H \times K$ mapping hk to the ordered pair (h, k).
   - It is a group homomorphism because if $g = hk$ and $g' = h'k'$ then $\varphi(gg') = \varphi(hkh'k') = \varphi(hh'kk') = (hh', kk') = \varphi(hk)\varphi(h'k') = \varphi(g)\varphi(g')$, where we used the fact that h' and k commute.
   - Finally, φ is trivially injective (since $(h, k) = (e, e)$ implies $hk = e$) and surjective (by definition of HK) and so it is an isomorphism.

Products of Subgroups, XIV

A brief interjection about some terminology in this last situation.

- If both H and K are normal in G, and $H \cap K = \{e\}$, then HK is isomorphic to the direct product $H \times K$.
- Under these hypotheses, we call the subgroup HK the internal direct product of H and K, and call the group $H \times K$ the external direct product of H and K.
- The difference is irrelevant as a practical matter, but the distinction is that the internal direct product is defined inside a group that already contains H and K as subgroups, whereas the external direct product is an explicit construction of a new group using the Cartesian product.

Products of Subgroups, XV

Proofs:

6. If $n_p = 1$ for every prime p dividing $\#G$, then G is the (internal) direct product of its Sylow subgroups.
   - The intersection of two Sylow subgroups with different primes is trivial by Lagrange's theorem, since the order of their intersection divides the order of each group.
   - Therefore, since they are all normal since $n_p = 1$ for every prime p dividing $\#G$, by applying (5) repeatedly we see that the product of any number of the Sylow subgroups is isomorphic to their direct product.
   - In particular, since the product of all the Sylow subgroups has the same order as G, it is equal to G, and so G is isomorphic to the direct product of its Sylow subgroups.

A group satisfying the condition (6) is called a nilpotent group.

Products of Subgroups, XV

One common technique for analyzing the structure of finite groups is to start with the various Sylow subgroups, and then take various products or normalizers to construct larger subgroups in terms of these.

- In particular, if we can show that all of the Sylow numbers are equal to 1, then the group is the direct product of its Sylow subgroups.
- This reduces us to the situation of having to identify all the possibilities for the Sylow subgroups.

Products of Subgroups, XVI

Example: Show that every group of order 7007 is abelian, and classify them up to isomorphism.

Products of Subgroups, XVI

Example: Show that every group of order 7007 is abelian, and classify them up to isomorphism.

- We start by finding the possible Sylow numbers.
- For a group of order $7007 = 7^2 \cdot 11 \cdot 13$, the number n_7 is congruent to 1 modulo 7 and divides $11 \cdot 13$. The only such number is 1, so $n_7 = 1$.
- Likewise, $n_{11} \equiv 1 \pmod{11}$ and divides $7^2 \cdot 13$, but the only such divisor is 1. Similarly, the only possible value for n_{13} is 1.

Products of Subgroups, XVI

Example: Show that every group of order 7007 is abelian, and classify them up to isomorphism.

- All of the Sylow subgroups of G are normal, so G is nilpotent and is the direct product of its Sylow subgroups.
- All of these Sylow subgroups are abelian since their orders are either a prime or a square of a prime, so G is abelian.
- By our classification of abelian groups, we see there are two isomorphism types for G: either $G \cong (\mathbb{Z}/49\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z}) \times (\mathbb{Z}/13\mathbb{Z}) \cong \mathbb{Z}/7007\mathbb{Z}$ or $G \cong (\mathbb{Z}/7\mathbb{Z}) \times (\mathbb{Z}/7\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z}) \times (\mathbb{Z}/13\mathbb{Z}) \cong (\mathbb{Z}/7\mathbb{Z}) \times (\mathbb{Z}/1001\mathbb{Z})$.

Products of Subgroups, XVII

For certain classes of group orders with a small number of prime divisors, we can essentially classify groups of that order using Sylow's theorems.

- We can illustrate some of the ideas by classifying the groups of order pq, where p and q are distinct primes.
- This will turn out to be more involved than it might seem in one case.

Groups of Order pq, I

Example: If p and q are primes with $p < q$ such that p does not divide $q - 1$, show that any group of order $n = pq$ is abelian and cyclic.

Groups of Order pq, I

<u>Example</u>: If p and q are primes with $p < q$ such that p does not divide $q - 1$, show that any group of order $n = pq$ is abelian and cyclic.

- By Sylow's theorems, the number n_p divides q and is congruent to 1 modulo p. Since p does not divide $q - 1$, the only possibility is $n_p = 1$.
- Likewise, n_q divides p and is congruent to 1 modulo q, so since $p < q$ we must have $n_q = 1$.
- Therefore, both the Sylow p-subgroup and the Sylow q-subgroup are normal in G, and so G is isomorphic to their direct product.
- Since both groups are cyclic, we see $G \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/pq\mathbb{Z}$ by the Chinese remainder theorem. Thus, G is cyclic as claimed.

Groups of Order pq, II

Of course, we have conspicuously omitted the case $q \equiv 1 \bmod p$.

- Indeed, at least in some cases we can see that the group is not necessarily abelian: for example, if $p = 2$, then we have the dihedral group $D_{2 \cdot q}$ of order $2q$, and it is not abelian.
- Thus, in this situation, it would seem that more is going on.
- Indeed, in addition to the case $n_p = n_q = 1$ (in which case G is cyclic by the above argument) there is also another possibility, namely, $n_p = q$.
- In this case, there are q total Sylow p-subgroups, each of which has $p - 1$ elements of order p for a total of $q(p - 1) = pq - q$ elements.
- Together with the q elements in the Sylow q-subgroup, this accounts for all of the elements in the group.

Groups of Order pq, III

We have not yet shown that there actually exists such a group.

- Undeterred, in this hypothetical group, let $P = \langle g \rangle$ be a Sylow p-subgroup, and $Q = \langle h \rangle$ be the Sylow q-subgroup.
- Then $PQ = G$ in this case by order considerations, even though G is not isomorphic to the direct product $P \times Q$.
- Observe that g acts on the set of elements of Q by conjugation, since Q is normal in G.
- Thus, $ghg^{-1} = h^d$ for some positive integer d.
- Moreover, since g has order p, we see $h = g^p h g^{-p} = h^{d^p}$, and so $d^p \equiv 1 \pmod{q}$.
- This means d must be an element of order p in $(\mathbb{Z}/q\mathbb{Z})^\times$, since d cannot equal 1 by the assumption that g and h do not commute. Note that such an element exists in $(\mathbb{Z}/q\mathbb{Z})^\times$, since $(\mathbb{Z}/q\mathbb{Z})^\times$ is cyclic (as we proved) and p divides its order $q-1$.

Groups of Order pq, IV

Our calculations on the last slide suggest that we could take a presentation of this group as $\langle g, h \,|\, g^p = h^q = e,\, ghg^{-1} = h^d \rangle$ where d is an element of order p in $(\mathbb{Z}/q\mathbb{Z})^\times$.

- It may seem that we would obtain several different groups, one for each of the $p-1$ elements of order p in $(\mathbb{Z}/q\mathbb{Z})^\times$.
- But in fact, they are all isomorphic to one another, as can be seen by changing variables from g to g^a for an appropriate value of $a \in (\mathbb{Z}/p\mathbb{Z})^\times$.

Groups of Order pq, V

We still need to show that $\langle g, h \,|\, g^p = h^q = e,\, ghg^{-1} = h^d \rangle$ actually does describe a group of order pq.

- Observe that by using the given relations, each element of the group is of the form $g^a h^b$ for some $a \in \{0, 1, \ldots, p-1\}$ and $b \in \{0, 1, \ldots, q-1\}$, so the order of the group is at most pq.
- To show equality, we can give a construction of such a group, motivated by the left-multiplication action of G on the elements of Q.
- This action is transitive and faithful, so if we label the elements $\{e, h, h^2, \ldots, h^{q-1}\}$ of Q as $\{1, 2, \ldots, q\}$, then the permutation associated to h is $(1\,2\,3\,\ldots\,q)$, while the permutation associated to g is the product of $(q-1)/p$ p-cycles that conjugates h to h^d.

Groups of Order pq, VI

<u>Examples</u>:

1. Suppose $p = 2$ and $q = 5$.
   - We take a q-cycle $h = (1\,2\,3\,4\,5)$.
   - Notice that -1 has order $p = 2$ in $(\mathbb{Z}/5\mathbb{Z})^{\times}$.
   - So we require $ghg^{-1} = h^{-1} = (1\,5\,4\,3\,2)$.
   - Thus, we can take $g = (2\,5)(3\,4)$.
2. Suppose $p = 3$ and $q = 7$.

Groups of Order pq, VI

Examples:

1. Suppose $p = 2$ and $q = 5$.
   - We take a q-cycle $h = (1\,2\,3\,4\,5)$.
   - Notice that -1 has order $p = 2$ in $(\mathbb{Z}/5\mathbb{Z})^\times$.
   - So we require $ghg^{-1} = h^{-1} = (1\,5\,4\,3\,2)$.
   - Thus, we can take $g = (2\,5)(3\,4)$.
2. Suppose $p = 3$ and $q = 7$.
   - We take a q-cycle $h = (1\,2\,3\,4\,5\,6\,7)$.
   - Notice that 2 has order $p = 3$ in $(\mathbb{Z}/7\mathbb{Z})^\times$.
   - So we require $ghg^{-1} = h^2 = (1\,3\,5\,7\,2\,4\,6)$.
   - Thus, we can take $g = (2\,3\,5)(4\,7\,6)$.

Groups of Order pq, VII

Examples:

3. Suppose $p = 5$ and $q = 11$.

Groups of Order pq, VII

Examples:

3. Suppose $p = 5$ and $q = 11$.
   - We take a q-cycle $h = (1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11)$.
   - Notice that 3 has order $p = 5$ in $(\mathbb{Z}/11\mathbb{Z})^{\times}$.
   - So we require $ghg^{-1} = h^3 = (1\,4\,7\,10\,2\,5\,8\,11\,3\,6\,9)$.
   - Thus, we can take $g = (2\,4\,10\,6\,5)(3\,7\,8\,11\,9)$.

Groups of Order pq, VIII

We can also give a construction using matrix groups.

- Specifically, take $H = \left\{ \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix} : x, y \in \mathbb{F}_q \text{ with } x^p = 1 \right\}$, the subgroup of upper-triangular matrices in $GL_2(\mathbb{F}_q)$ whose diagonal entries are $\{x, 1\}$ where $x^p = 1$.
- Since $\mathbb{F}_q^\times$ is cyclic of order $q - 1$ as we showed, and p divides $q - 1$, the kernel of the pth power map has order p, so there are p possible values of x.
- Since there are q possible values of y, we see $\#H = pq$.
- Now we just have to show it has the desired presentation.

Groups of Order pq, IX

We have $H = \left\{ \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix} : x, y \in \mathbb{F}_q \text{ with } x^p = 1 \right\}$.

- By order considerations, H is generated by the elements $\tilde{g} = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}$ of order p, where a is a primitive pth root of unity, and $\tilde{h} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ of order q.
- It is then a straightforward calculation to see that $\tilde{g}^p = \tilde{h}^q = I_2$ and $\tilde{g}\tilde{h}\tilde{g}^{-1} = \tilde{h}^a$.
- Thus, H has the desired presentation $\langle g, h \,|\, g^p = h^q = e,\, ghg^{-1} = h^d \rangle$, and is the unique non-abelian group of order pq up to isomorphism.

Groups of Order p^2q, I

Using similar arguments we can classify groups of order p^2q for certain values of p and q.

- Specifically, if p and q are distinct primes, we will show that any group G of order p^2q must have a normal Sylow p-subgroup or a normal Sylow q-subgroup.
- Furthermore, if p does not divide $q-1$ and $(p,q) \neq (2,3)$, we can show that G must be abelian and isomorphic to $\mathbb{Z}/p^2q\mathbb{Z}$ or to $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/pq\mathbb{Z})$.

Groups of Order p^2q, II

First, we analyze the possible Sylow numbers for G of order p^2q.

- If $p > q$ then $n_p \in \{1, q\}$ but it cannot equal q because $q \not\equiv 1 \pmod{p}$. Thus in this case, $n_p = 1$.
- Otherwise, suppose $p < q$. Then $n_p \in \{1, q\}$ and $n_q \in \{1, p^2\}$ since $n_q \neq p$ because $p < q$ and so p cannot be congruent to 1 modulo q.
- If $n_q = p^2$ then there would be $p^2(q-1)$ elements of order q in these Sylow q-subgroups, leaving only $n - p^2(q-1) = p^2$ elements left for the Sylow p-subgroup, so n_p would be 1.
- Therefore, G also must have a normal Sylow subgroup in this case.

Groups of Order p^2q, III

In fact, we can say more.

- Indeed, when $p < q$, if p does not divide $q - 1$ then we cannot have $n_p = q$, so $n_p = 1$.
- Furthermore, if we had $n_q = p^2$, then $p < q$ and q divides $p^2 - 1$.
- But since q is prime, either q divides $p - 1$ (impossible since $p < q$) or q divides $p + 1$.
- But because $p < q$, the only possibility is that $q = p + 1$.
- Since the only even prime is 2, this forces $p = 2$ and $q = 3$, which we specifically excluded.
- Therefore, we have $n_p = n_q = 1$.

Groups of Order p^2q, IV

So, if $(p, q) \neq (2, 3)$ and q is not 1 mod p, we have $n_p = n_q = 1$.

- Then, G is nilpotent hence isomorphic to the direct product of its Sylow p-subgroup and its Sylow q-subgroup.
- Since both of these Sylow subgroups are abelian since their orders are either a prime or a square of a prime, we see that G is abelian.
- Then by the classification of finitely generated abelian groups, G is a direct product of cyclic groups, and based on its prime factorization we get the two possibilities $\mathbb{Z}/p^2q\mathbb{Z}$ and $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/pq\mathbb{Z})$ given above.

Groups of Order p^2q, V

It remains to analyze the situations of groups of order 12, and the situation where only one of the Sylow subgroups is normal.

- Much like the situation with groups of order pq, we will be able to construct non-abelian groups in these cases.
- We would like to do this more systematically than the fairly ad hoc approach we took with groups of order pq.
- We will therefore finish off this chapter by discussing semidirect products, which will allow us to write down more general constructions for groups in exactly these situations.

Motivation for Semidirect Products, I

Suppose we have subgroups H and K of a group G, such such that $G = HK$ and $H \cap K = \{e\}$, but now we only assume H is normal, not necessarily K.

- As a prototypical example, think of $H = \langle r \rangle$ and $K = \langle s \rangle$ inside $D_{2 \cdot n}$.
- Then since $G = HK$ and $H \cap K = \{e\}$, every element of G must be uniquely written in the form hk for $h \in H$ and $k \in K$, since the number of such products is $\#H \cdot \#K = \#G$.
- It is no longer true, however, that elements of H will commute with elements of K, so in order to describe the multiplication in this group, we need to be able to convert a product $(h_1 k_1) \cdot (h_2 k_2)$ into a product of an element of H with an element of K.

Motivation for Semidirect Products, II

Since $HK = G$ is a subgroup of G, we know that $HK = KH$.

- So, the element $k_1 h_2 \in KH$ must be of the form $h_3 k_3 \in HK$. Then we can write $(h_1 k_1) \cdot (h_2 k_2) = h_1(k_1 h_2)k_2 = h_1(h_3 k_3)k_2 = (h_1 h_3)(k_3 k_2) \in HK$.
- It is not so clear what precisely we can do to simplify this procedure.
- For motivation, consider $D_{2 \cdot n}$: whenever we want to simplify a product like $(sr^2)(sr^5)$, we use the relation $rs = sr^{-1}$.
- Now notice that we can rewrite that relation as $srs^{-1} = r^{-1}$.
- The point here is that $H = \langle r \rangle$ is normal, so the elements of K will act on it by conjugation. So in fact we will always get a relation of this kind when H is normal.

Motivation for Semidirect Products, III

For each $k \in K$, it is true that $kHk^{-1} = H$, since H is normal.

- Thus, for each $k \in K$, we have an associated isomorphism $\varphi_k : H \to H$ with $\varphi_k(h) = khk^{-1}$.
- We can use this to evaluate the product $(h_1 k_1) \cdot (h_2 k_2)$.
- Specifically, we have $k_1 h_2 = \varphi_{k_1}(h_2) k_1$, and therefore $(h_1 k_1) \cdot (h_2 k_2) = h_1 [k_1 h_2] k_2 = h_1 [\varphi_{k_1}(h_2) k_1] k_2$ $= [h_1 \varphi_{k_1}(h_2)] \cdot [k_1 k_2]$.
- What we see is that if we work with ordered pairs $(h, k) \in H \times K$, then the composition operation we have is $(h_1, k_1) \star (h_2, k_2) = (h_1 \varphi_{k_1}(h_2), k_1 k_2)$: it behaves as normal multiplication in the K-component, but it is "twisted" by the isomorphism φ_{k_1} in the H-component.

Motivation for Semidirect Products, IV

Let's work out exactly what this looks like in $G = D_{2 \cdot 5}$, with $H = \langle r \rangle = \{e, r, r^2, r^3, r^4\}$ and $K = \langle s \rangle = \{e, s\}$.

- For each element of K, we get an isomorphism $\varphi_k : H \to H$ acting via $\varphi_k(h) = khk^{-1}$.
- So, the isomorphism φ_e has $\varphi_e(h) = ehe^{-1} = h$, so it is just the identity.
- The isomorphism φ_s has $\varphi_s(h) = shs^{-1} = h^{-1}ss^{-1} = h^{-1}$ for each $h \in H$, and so φ_s is the map taking each element of H to its inverse.
- Using the ordered pair notation, for example, we get $(r, s) \star (r^2, e) = (r\varphi_s(r^2), se) = (r \cdot r^{-2}, se) = (r^4, s)$, which, in regular notation inside G, reads as the statement $(rs)(r^2) = r^4 s$, which is indeed true.

Motivation for Semidirect Products, V

As we have noted previously, the isomorphisms of H with itself are called automorphisms.

- Conveniently, someone put a problem on Homework 8 that was all about group automorphisms, so (presumably) you're now at least moderately comfortable with them.
- As you showed, the automorphisms of H form a group under function composition, denoted $\mathrm{Aut}(H)$.
- So: for each element of K we have an automorphism φ_k of H.
- Furthermore, we have $\varphi_{kk'} = \varphi_k \circ \varphi_{k'}$ for any $k, k' \in K$, since $\varphi_{kk'}(h) = (kk')h(kk')^{-1} = \varphi_k(\varphi_{k'}(h))$ for all $h \in H$.
- This means that the association of k to the map φ_k is actually a group homomorphism of K into $\mathrm{Aut}(H)$.

Motivation for Semidirect Products, VI

The idea now is that we can reverse this process.

- Explicitly, suppose that H and K are any groups and we have a homomorphism σ of K into $\mathrm{Aut}(H)$, so that for each $k \in K$ we obtain an automorphism σ_k of H.
- We can then use the calculations we just made on the last slides to *define* a group operation $\star$ on ordered pairs (h, k) by taking $(h_1, k_1) \star_\sigma (h_2, k_2) = (h_1 \sigma_{k_1}(h_2),\ k_1 k_2)$.
- Of course, we do have to check that this is actually a group, but it is.
- The resulting group is called the semidirect product of H and K.

Semidirect Products, I

Theorem (Semidirect Products)

Let H and K be any groups, let $\sigma : K \to \mathrm{Aut}(H)$ be a group homomorphism with σ_k being the automorphism $\sigma(k)$ on H, and let G be the set of ordered pairs (h, k) for $h \in H$ and $k \in K$. Then G is a group with order $\#H \cdot \#K$ under the operation

$$(h_1, k_1) \star_\sigma (h_2, k_2) = (h_1 \sigma_{k_1}(h_2),\ k_1 k_2).$$

Furthermore, the subset $\{(h, e) : h \in H\}$ is isomorphic to H and is a normal subgroup of G, while the subset $\{(e, k) : k \in K\}$ is isomorphic to K.
This group is called the <u>semidirect product</u> of H and K with respect to σ, and is denoted $H \rtimes_\sigma K$.

Semidirect Products, II

Proof:

- Each of the assertions is a direct calculation.
- For [G1], first note that $\sigma_{k_1 k_2}(h_3) = \sigma_{k_1}(\sigma_{k_2}(h_3))$.
- Then we have

$$\begin{aligned}
&[(h_1, k_1) \star_\sigma (h_2, k_2)] \star_\sigma (h_3, k_3) \\
&\quad = (h_1 \sigma_{k_1}(h_2),\ k_1 k_2) \star_\sigma (h_3, k_3) \\
&\quad = (h_1 \sigma_{k_1}(h_2) \sigma_{k_1 k_2}(h_3),\ k_1 k_2 k_3) \\
&\quad = (h_1 \sigma_{k_1}(h_2) \sigma_{k_1}(\sigma_{k_2}(h_3)),\ k_1 k_2 k_3) \\
&\quad = (h_1 \sigma_{k_1}(h_2 \sigma_{k_2}(h_3)),\ k_1 k_2 k_3) \\
&\quad = (h_1, k_1) \star_\sigma (h_2 \sigma_{k_2}(h_3),\ k_2 k_3) \\
&\quad = (h_1, k_1) \star_\sigma [(h_2, k_2) \star_\sigma (h_3, k_3)].
\end{aligned}$$

Semidirect Products, III

Proof (continued):

- For [G2], we observe that (e, e) is the identity of G, since $(e, e) \star_\sigma (h, k) = (e\sigma_e(h),\ ek) = (h, k)$ and likewise $(h, k) \star_\sigma (e, e) = (h, k)$.
- For [G3], the inverse of (h, k) is $(\sigma_{k^{-1}}(h^{-1}), k^{-1})$, since $(h, k) \star_\sigma (\sigma_{k^{-1}}(h^{-1}), k^{-1}) = (h\sigma_k(\sigma_{k^{-1}}(h^{-1})), kk^{-1}) = (e, e)$ and likewise $(\sigma_{k^{-1}}(h^{-1}), k^{-1}) \star_\sigma (h, k) = (e, e)$.
- Also, $\{(h, e)\ :\ h \in H\}$ is a normal subgroup isomorphic to H, since $(h_1, e) \star (h_2, e) = (h_1 h_2, e)$ and $(h_1, k) \star (h_2, e) \star (h_1, k)^{-1} = (h_1 h_2 h_1^{-1}, e)$.
- Likewise, $\{(e, k)\ :\ k \in K\}$ is a subgroup isomorphic to K, since $(e, k_1) \star (e, k_2) = (e, k_1 k_2)$.

Semidirect Products, IV

The idea here is that semidirect products are somewhat like direct products (whose underlying set is also ordered pairs of elements of H and K) but have a different group operation.

- In fact, if σ is the identity map, then the semidirect product with respect to σ is simply the direct product, since the group operation is $(h_1, k_1) \star_\sigma (h_2, k_2) = (h_1 \sigma_{k_1}(h_2),\ k_1 k_2)$.
- Furthermore, we can view H and K as being embedded inside of the semidirect product $H \rtimes_\sigma K$ as the subgroups $\{(h, e) : h \in H\}$ and $\{(e, k) : k \in K\}$ respectively.
- When we make this identification, we see that $H \cap K = \{e\}$, $G = HK$, and H is a normal subgroup of G: this is precisely the setup we started with.

Semidirect Products, V

The point of all of this discussion was to identify when we can decompose a group G as a semidirect product.

- Specifically, if we can decompose G as a product HK for two subgroups H and K with H normal in G and $H \cap K = \{e\}$, this means G must be (isomorphic to) a semidirect product $H \rtimes_\sigma K$ for some $\sigma : K \to \mathrm{Aut}(H)$.
- As with direct products, in principle we should draw a distinction between an internal semidirect product (in which we already have a group G with those subgroups H and K as above) and an external semidirect product (in which we are taking two abstract groups H and K with some $\sigma \to \mathrm{Aut}(H)$ and constructing this new group $H \rtimes_\sigma K$).
- In practice, we don't really care, since we are thinking of the semidirect product as an abstract construction most of the time anyway.

Semidirect Products, VI

A few miscellaneous notational remarks:

- The notation $H \rtimes_\sigma K$ is intended to evoke the direct product but also to point out the asymmetry between H (which is normal) and K (which need not be).
- The side of the symbol $\rtimes$ with the vertical bar identifies the subgroup that is not normal.
- Contrarians sometimes use $A \ltimes_\sigma B$, which is a semidirect product in which B is normal, and $\sigma : A \to \mathrm{Aut}(B)$.
- One may always switch the order in this way because if $AB = G$ then $BA = G$ as well (since BA is a subgroup, it equals AB), though the resulting construction differs slightly.
- When the map σ is clear from context, it is often omitted. Usually, when we write $H \rtimes K$ with no σ, we are specifically avoiding the case where we end up with the direct product.

Semidirect Products, VII

Examples:

1. Let $H = \langle a \rangle$ be cyclic of order 5 and $K = \langle b \rangle$ be cyclic of order 4.
   - Let $\sigma : K \to \mathrm{Aut}(H)$ be the homomorphism such that $\sigma_b(a) = a^2$.
   - Note that there is such a homomorphism, because the squaring map has order 4 inside $\mathrm{Aut}(H) \cong (\mathbb{Z}/5\mathbb{Z})^\times$, which is cyclic of order 4 and generated by the element 2.
   - The resulting semidirect product $H \rtimes_\sigma K$ is a group of order 20 generated by a and b.
   - The elements a, b satisfy the relations $a^5 = e$ and $b^4 = e$ inherited from H and K, and they also satisfy $bab^{-1} = a^2$ from the action of the automorphism.
   - We get a presentation $\left\langle a, b \mid a^5 = b^4 = e,\ bab^{-1} = a^2 \right\rangle$.

Semidirect Products, VII

Examples:

2. Let $H = \langle a \rangle$ be cyclic of order 5 and $K = \langle b \rangle$ be cyclic of order 4.
   - We can construct a different semidirect product if instead we use the homomorphism $\tau : K \to \mathrm{Aut}(H)$ such that $\sigma_b(a) = a^4$. This is well-defined because this automorphism has order 2 inside $\mathrm{Aut}(H)$.
   - Then $H \rtimes_\sigma K$ is a group of order 20 generated by a and b, but now a, b satisfy the relations $bab^{-1} = a^4 = a^{-1}$, so this group has a presentation $\left\langle a, b \,\middle|\, a^5 = b^4 = e,\ bab^{-1} = a^{-1} \right\rangle$.

Semidirect Products, VIII

In these two examples, we have constructed two groups of order 20.

- The two semidirect products we constructed were $G_1 = \langle a, b \mid a^5 = b^4 = e,\ bab^{-1} = a^2 \rangle$ and $G_2 = \langle a, b \mid a^5 = b^4 = e,\ bab^{-1} = a^{-1} \rangle$.
- In fact, these are different from any of the other groups of order 20 we have encountered so far.
- Neither of them is abelian, like $\mathbb{Z}/20\mathbb{Z}$ and $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/10\mathbb{Z})$, and neither is isomorphic to the dihedral group $D_{2\cdot 10}$ since the dihedral group has no elements of order 4.
- G_1 and G_2 are also not isomorphic to each other, although this is a bit harder to see directly: one way is to note that the second group has an element of order 5 and order 2 that commute (namely, a and b^2) while the first doesn't.
- It is easier to note that the images $\mathrm{im}(\sigma)$ for $\sigma : K \to \mathrm{Aut}(H)$ differ for these two groups (G_1 has order 4, G_2 has order 2).

Semidirect Products, IX

Examples:

3. Let H be any abelian group and $K = \langle b \rangle$ be cyclic of order 2.
   - Also let $\sigma : K \to \mathrm{Aut}(H)$ be the map sending the nonidentity element $b \in K$ to the inversion automorphism with $\sigma_b(a) = a^{-1}$ for any $a \in H$.
   - We obtain a semidirect product $H \rtimes_\sigma K$ of order $2 \cdot \#H$.
   - If $H = \langle a \rangle$ is cyclic of order n, then the resulting semidirect product is a group of order $2n$ generated by a and b, and a, b satisfy the relations $bab^{-1} = a^{-1}$.
   - In that case, the semidirect product is isomorphic to the dihedral group $D_{2 \cdot n}$, with a playing the role of r and b playing the role of s.
   - However, for other H, we get new groups. For example, if H is isomorphic to $\mathbb{Z}$, we get a group with presentation $\langle a, b \mid b^2 = e, bab^{-1} = a^{-1} \rangle$.

Semidirect Products, IX

Examples:

4. Let $H = \langle a \rangle$ be cyclic of order q and $K = \langle b \rangle$ be cyclic of order p, for primes p and q.
   - Then to construct a semidirect product $H \rtimes_\sigma K$, we need a map $\sigma : K \to \mathrm{Aut}(H)$.
   - Note that $\mathrm{Aut}(H) \cong (\mathbb{Z}/q\mathbb{Z})^\times$ is cyclic of order $q - 1$.
   - So if p does not divide $q - 1$, the only such map σ is the identity map, yielding the direct product.
   - If p does divide $q - 1$, then there is a nontrivial map σ, since $\mathrm{Aut}(H)$ will contain an element d of order p.
   - If we take $\sigma_b(a) = a^d$, then the semidirect product has presentation $\langle a, b \,|\, a^q = b^p = e, bab^{-1} = a^d \rangle$, which is the non-abelian group of order pq we found earlier.

Semidirect Products, X

In fact, we could have used semidirect products to classify the groups of order pq quite a bit more simply[1].

- Explicitly, if $p < q$ then we know the Sylow q-subgroup H is normal. Then if K is any Sylow p-subgroup, we have $H \cap K = \{e\}$ by Lagrange's theorem, and so $HK = G$.
- This tells us that G is a semidirect product $H \rtimes_\sigma K$ for some $\sigma : K \to \mathrm{Aut}(H)$.
- The analysis we just gave then shows G is actually a direct product unless p divides $q - 1$, in which case there are some nontrivial possible σ, which yield non-abelian groups.
- Using a result we will mention next time, all of those groups turn out to be isomorphic.

[1] In fact, we really did just write down the semidirect product structure, just without identifying it as such.

Summary

We discussed products of subgroups and established some of their basic properties.

We classified groups of some orders.

We introduced semidirect products.

Next lecture: More semidirect products, field automorphisms.