

NOTES ON SEMIDIRECT PRODUCTS

Since semidirect products are not discussed in the text, here are some notes on them.

1. DIRECT PRODUCTS

Let G be a group and H and K subgroups satisfying:

$$H \text{ and } K \text{ are normal in } G, \quad H \cap K = \{1\}, \quad HK = G.$$

In this case you proved in a homework and we then proved in class that G is isomorphic to the *direct product* $H \times K$. Since we are happy to think of groups that are isomorphic as “essentially the same” we will simply say that G is the direct product of H and K .

2. SEMIDIRECT PRODUCTS

Suppose now we relax the first condition, so that H is still normal in G but K need not be. We retain the other conditions, so our conditions are now:

- (1) H is normal in G ,
- (2) $H \cap K = \{1\}$,
- (3) $HK = G$,

In this case we obtain what is called a *semidirect product*.

Examples: Suppose $H \cong \mathbb{Z}/3$ and $K \cong \mathbb{Z}/2$. There is more than one possibility for G :

- (i) If K is also normal in G then we already know $G \cong H \times K$, which is abelian and isomorphic to $\mathbb{Z}/6$.
- (ii) On the other hand K might not be normal in G , for example G might be the symmetric group S_3 , with $H = \{(1), (123), (132)\}$ and $K = \{(1), (12)\}$.

The above examples show that for given H and K there may be more than one semidirect product. Thus, unlike for the direct product, the groups H and K may not alone give enough information to recover the structure of the group G . The extra information we need consists of a homomorphism from K to the group of automorphisms of H :

$$\phi: K \rightarrow \text{Aut}(H).$$

This may seem a bit intimidating at first, but I hope that it will become less so once we have some examples. First we'll describe where this $\phi: K \rightarrow \text{Aut}(H)$ comes from. A remark on notation: for $k \in K$ we would have to write $\phi(k)(h)$ for the result of applying the automorphism $\phi(k)$ to the

element $h \in H$. This notation is a bit confusing, so we will write ϕ_k instead of $\phi(k)$.

For $k \in K$ we define the automorphism ϕ_k to be the automorphism of H given by conjugation:

$$\phi_k : H \rightarrow H, \quad \phi_k(h) = khk^{-1}.$$

We need to show this really gives a homomorphism:

Theorem 1. *The map $k \mapsto \phi_k$ is a homomorphism $\phi: K \rightarrow \text{Aut}(H)$.*

Proof. We must show $\phi_{k_1}\phi_{k_2} = \phi_{k_1k_2}$ for any $k_1, k_2 \in K$. Note that $\phi_{k_1}\phi_{k_2}$ and $\phi_{k_1k_2}$ are functions in their own right (they are maps $H \rightarrow H$) and to show two functions are equal we have to show they take the same value on any element h of H . That is, we need to show

$$\phi_{k_1}\phi_{k_2}(h) = \phi_{k_1k_2}(h)$$

for any $h \in H$. The left side of this equation is

$$\phi_{k_1}\phi_{k_2}(h) = \phi_{k_1}(k_2hk_2^{-1}) = k_1k_2hk_2^{-1}k_1^{-1}.$$

The right side is

$$\phi_{k_1k_2}(h) = k_1k_2h(k_1k_2)^{-1} = k_1k_2hk_2^{-1}k_1^{-1}.$$

These are equal, so the proof is complete. \square

Next we show that if we know the groups H , K and the homomorphism ϕ then we can recover the group structure of the group G .

Since $G = HK$, every element of G can be written in the form hk with $h \in H$ and $k \in K$. Moreover, it has a unique such expression. (*Proof:* if $h_1k_1 = h_2k_2$ then $h_2^{-1}h_1 = k_2k_1^{-1}$. Since $h_2^{-1}h_1 \in H$ and $k_2k_1^{-1} \in K$ and $H \cap K = \{1\}$, we see that $(h')^{-1}h = k'k^{-1} = 1$, so $h = h'$ and $k = k'$.)

Given any two elements hk and $h'k'$ of G , we want to know how to write their product and the inverse of hk in the same form.

Theorem 2. *If $h, h' \in H$ and $k, k' \in K$ then*

$$hk h'k' = h''k'' \text{ with } h'' = h\phi_k(h') \text{ and } k'' = kk'$$

$$\text{and } (hk)^{-1} = \phi_{k^{-1}}(h^{-1})k^{-1}.$$

Proof. $hkh'k' = hkh'(k^{-1}k)k' = h(kh'k^{-1})kk' = h\phi_k(h')kk'$ and $(hk)^{-1} = k^{-1}h^{-1} = k^{-1}h^{-1}kk^{-1} = \phi_{k^{-1}}(h^{-1})k^{-1}$. \square

So we have seen that to determine the group structure of a semidirect product, the information we need are the groups K and H together with the homomorphism $\phi: K \rightarrow \text{Aut}(H)$. Conversely, if we start with groups H and K and a homomorphism

$$\phi: K \rightarrow \text{Aut}(H) \text{ given by } k \mapsto \phi_k,$$

we can ask if there always is some semidirect product group based on this information. The answer is “yes”:

Theorem 3. *Given groups H and K and a homomorphism $K \rightarrow \text{Aut}(H)$ there is a semidirect product group G based on this information. We can construct it as follows. The underlying set of G is the set of pairs (h, k) with $h \in H$ and $k \in K$. The multiplication on this set is given by the rule*

$$(h, k)(h', k') = (h\phi_k(h'), kk'),$$

the identity element is $(1, 1)$, and inverse is given by

$$(h, k)^{-1} = (\phi_{k^{-1}}(h^{-1}), k^{-1}).$$

Once we have shown (see below) that this rule defines a group it is more convenient to introduce the shorthand hk for (h, k) and think of H and K as subgroups of G , just as we have done earlier for the direct product. This semidirect product is denoted

$$G = H \rtimes K.$$

Note that the symbol \rtimes is a combination of the normal subgroup symbol \triangleleft and the product symbol \times and the notation tells one which of H and K is the normal subgroup (one can also write $K \rtimes H$ for the same group). This notation is not really satisfactory, since the structure depends not only on H and K but also on the homomorphism $\phi : K \rightarrow \text{Aut}(H)$. One sometimes writes $G = H \rtimes_{\phi} K$ to include all the necessary information in the notation.

Proof of the theorem. We must check that multiplication is associative, and the identity and inverse laws hold. It is good practice to try to write out this proof for yourself without reference to the proof below. Anyway, here is the proof of associativity:

$$\begin{aligned} ((h, k)(h', k'))(h'', k'') &= (h\phi_k(h'), kk')(h'', k'') \\ &= (h\phi_k(h')\phi_{kk'}(h''), kk'k'') \\ &= (h\phi_k(h')(\phi_k \circ \phi_{k'})(h''), kk'k'') \\ &= (h\phi_k(h')\phi_k(\phi_{k'}(h'')), kk'k'') \\ &= (h\phi_k(h'\phi_{k'}(h'')), kk'k'') \\ &= (h, k)(h'\phi_{k'}(h''), k'k'') \\ &= (h, k)((h', k')(h'', k'')) \end{aligned}$$

Identity:

$$(h, k)(1, 1) = (h\phi_k(1), k) = (h, k), \quad (1, 1)(h, k) = (1\phi_1(h), k) = (h, k).$$

Inverse:

$$(h, k)(\phi_{k^{-1}}(h^{-1}), k^{-1}) = (h\phi_k(\phi_{k^{-1}}(h^{-1})), kk^{-1}) = (hh^{-1}, kk^{-1}) = (1, 1).$$

We thus have a group. We still have to show that it is the desired semidirect product of H and K . We have injective maps

$$H \rightarrow G \text{ given by } h \mapsto (h, 1), \text{ and } K \rightarrow G \text{ given by } k \mapsto (1, k).$$

and both are homomorphisms since

$$(h, 1)(h', 1) = (h\phi_1(h'), 1) = (hh', 1), \text{ and } (1, k)(1, k') = (1\phi_k(1), kk') = (1, kk').$$

These injective homomorphisms let us think of H and K as subgroups of G . It is clear that $H \cap K = \{(1, 1)\}$ and $HK = G$ since $(h, 1)(1, k) = (h, k)$.

Finally, we must show that H is normal in G and that the action of K on H by conjugation in G is given by the original homomorphism ϕ . Both follow from the calculation: $(1, k)(h, 1)(1, k)^{-1} = (1, k)(h, 1)(1, k^{-1}) = (\phi_k(h), k)(1, k^{-1}) = (\phi_k(h), 1)$. \square

3. APPLICATIONS

With the semidirect product we can now classify all groups of order pq where p and q are primes with $q < p$.

Let H be a Sylow p -subgroup and K a Sylow q -subgroup of G . H is cyclic of order p and K is cyclic of order q . The number of Sylow p -subgroups is a divisor of q which is congruent to 1 mod p . 1 is the only possibility since $q < p$. Thus $H \trianglelefteq G$.

$H \cap K = \{1\}$ since it is a group of order dividing both p and q .

Since $H \trianglelefteq G$, we know HK is a subgroup of G . It has H and K as subgroups, so its order is divisible by both p and q , so $HK = G$.

Thus we have a semidirect product

$$G = H \rtimes K.$$

Which semidirect product is it? It can, of course be the direct product (this always exists, and corresponds to the case where the homomorphism $\phi : K \rightarrow \text{Aut}(H)$ is the trivial homomorphism). This gives $G \cong \mathbb{Z}_{pq}$. But if a non-trivial homomorphism $\phi : K \rightarrow \text{Aut}(H)$ exists then we also get a non-abelian group $G = H \rtimes_{\phi} K$ of order pq .

We shall see in class that $\text{Aut}(K) \cong \mathbb{Z}/(p-1)$. So a non-trivial homomorphism $K \rightarrow \text{Aut}(H)$ exists if and only if q divides $p-1$.

We will verify in class that there is then only one non-trivial homomorphism ϕ up to isomorphism, so we get just one non-abelian group $G = H \rtimes K$ of order pq . The final conclusion is thus:

Theorem 4. *If $q < p$ are prime numbers then either*

- $p \not\equiv 1 \pmod{q}$ and any group of order pq is cyclic, or
- $p \equiv 1 \pmod{q}$ and there are two groups of order pq up to isomorphism: the cyclic group and a non-abelian group $\mathbb{Z}_p \rtimes \mathbb{Z}_q$.

We can also classify groups of order p^2 :

Theorem 5. *If $|G| = p^2$ with p prime then G is abelian, so $G \cong \mathbb{Z}/p^2$ or $\mathbb{Z}/p \times \mathbb{Z}/p$.*

Proof. This is an exercise; start from the fact (which you proved in an earlier homework exercise) that the center $Z(G)$ of G is $\neq \{1\}$. Show that you are done if $Z(G) = G$, while if $Z(G) \neq G$ pick an element g outside $Z(G)$ and show that g and $Z(G)$ together must generate an abelian group and this abelian group must be G . \square

Example. We will construct the nonabelian group of order 6 as a semidirect product. Write its Sylow subgroups as

$$H = \{1, \sigma, \sigma^2\}, \quad K = \{1, \tau\}.$$

We need a non-trivial homomorphism $\phi : K \rightarrow \text{Aut}(H)$. Now there is just one non-trivial automorphism of H , namely the automorphism that exchanges the elements σ and σ^2 , so ϕ_{τ} must be this automorphism. G thus consists of the elements $1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau$ and Theorem 3 lets us fill in its group table (here is a start; you do the rest):

	1	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
1	1	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
σ						
σ^2						
τ	τ	$\sigma^2\tau$	$\sigma\tau$	1	σ^2	σ
$\sigma\tau$						
$\sigma^2\tau$						

At this point we can classify all groups of order < 27 with the exception of orders 8, 12, 16, 24. We will come back to order 8 later (there are two nonabelian ones, and you know how to list the three abelian ones, for a total of five).

We will sketch the classification of groups of order 12. There are exactly five of these up to isomorphism.

Let H be the 2-Sylow subgroup (of order 4) and K the 3-Sylow subgroup (of order 3). When one does the numerology one sees that neither H nor K is forced to be normal. H is isomorphic to one of $\mathbb{Z}/4$ and $\mathbb{Z}/2 \times \mathbb{Z}/2$ and K is isomorphic to $\mathbb{Z}/3$. There are thus several cases to try:

- (1) H and K both normal. This is the case that G is abelian. We get $G \cong \mathbb{Z}/12$ or $\mathbb{Z}/2 \times \mathbb{Z}/6$ according as whether H is $\mathbb{Z}/4$ or $\mathbb{Z}/2 \times \mathbb{Z}/2$.
- (2) $H \cong \mathbb{Z}_4$ normal, $K \cong \mathbb{Z}_3$ not normal;
- (3) $H \cong \mathbb{Z}_4$ not normal, $K \cong \mathbb{Z}_3$ normal;
- (4) $H \cong \mathbb{Z}_4$ not normal, $K \cong \mathbb{Z}_3$ not normal;
- (5) $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ normal, $K \cong \mathbb{Z}_3$ not normal;
- (6) $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ not normal, $K \cong \mathbb{Z}_3$ normal;
- (7) $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ not normal, $K \cong \mathbb{Z}_3$ not normal;

We shall discuss this in class. We shall see that case (2) does not occur (no nontrivial homomorphism $\phi : K \rightarrow \text{Aut}(H)$), and that each of cases (3), (5), (6) leads to a single possibility (up to isomorphism) for G . The resulting groups are a group we have not seen before, A_4 and $S_3 \times \mathbb{Z}_2$ respectively.

Finally, cases (4) and (7) do not occur. Here is one approach to see this: consider the action of G on the set of cosets of K ; show that this gives an injective homomorphism $G \rightarrow S_4$, then deduce a contradiction.