

## Semidirect products

Suppose the short exact sequence of groups

$$1 \rightarrow N \xrightarrow{\varphi} G \xrightarrow{\psi} H \rightarrow 1$$

"mapping of groups" = "homomorphism"

has a **splitting**, i.e. a mapping  $j: H \rightarrow G$  such that  $\psi \circ j = \text{id}_H$ .

Then  $j$  must be injective:  $j(h) = j(h') \Rightarrow \psi j(h) = \psi j(h') \Rightarrow h = h'$ .

Since  $\varphi$  is injective, it is an isomorphism onto its image, which is  $\ker \psi$ , hence normal in  $G$ . Letting  $H$  act on  $N$  by conjugation gives an automorphism of  $N$

$$\begin{aligned} \alpha: H &\longrightarrow \text{Aut}(N) & \text{where} \\ h &\longmapsto c_h \end{aligned}$$

$$\begin{aligned} c_h: N &\longrightarrow N \\ n &\longmapsto j(h) \varphi(n) j(h)^{-1} \end{aligned}$$

One may check that  $\alpha$  is a homomorphism of groups.

Example  $G = N \times H$

$$\begin{aligned}
 1 &\rightarrow N \xrightarrow{\alpha} N \times H \xrightarrow{\psi} H \rightarrow 1 \\
 n &\mapsto (n, 1) \\
 (n, h) &\mapsto h
 \end{aligned}$$

$$\begin{aligned}
 N \times H &\xleftarrow{j} H \\
 (1, h) &\xleftarrow{\quad} h
 \end{aligned}$$

In this case  $\alpha: H \rightarrow \text{Aut}(N)$  where  $c_h(n) = (1, h)(n, 1)(h, 1)^{-1} = (n, 1)$ .  
 $h \mapsto c_h$

Thus,  $\alpha(h) = \text{id}_N \quad \forall h \in H$ .

Example  $G = D_4 = \langle \phi, \rho : \phi^2 = \rho^4 = 1, \rho\phi = \phi\rho^3 \rangle, H = \langle \phi \rangle, N = \langle \rho \rangle$ .

$$\begin{aligned}
 1 &\rightarrow N \hookrightarrow G \rightarrow H \rightarrow 1 \\
 \rho &\mapsto 1 \\
 \phi &\mapsto \phi
 \end{aligned}$$

(Check this  $G \rightarrow H$  is a well-defined homomorphism. For instance,  $\rho\phi = \phi\rho^3$  and  $\rho\phi \mapsto \phi, \phi\rho^3 \mapsto \phi$ .)

The mapping  $j: H \rightarrow G$  gives a splitting.  
 $\phi \mapsto \phi$

The corresponding mapping  $H \rightarrow \text{Aut}(N)$  is given by  
 $h \mapsto c_h$  where  $c_h(n) = hnh^{-1}$ . The image of  $H$  here  
 consists of 2 automorphisms:  $c_1 = \text{id}_N$  and  $c_\phi = \text{conjugation by } \phi$ , and  
 $c_\phi(\rho^i) = \phi \rho^i \phi^{-1} = \phi \rho^i \phi = \rho^{3i}$ . Note that since  $N \cong \mathbb{Z}_4$ , a  
 cyclic group with 2 generators, 1 and 3, we get  $|\text{Aut}(N)| = 2$ . So  
 $H \rightarrow \text{Aut}(N)$  in this case is an isomorphism.

Now turn things around

Def. Let  $N$  and  $H$  be groups, and let  $\alpha: H \rightarrow \text{Aut}(N)$  be a homomorphism.  
 The **semidirect** product of  $N$  and  $H$  is the Cartesian product  $N \times H$  with  
 multiplication given by  $(n_1, h_1) \cdot (n_2, h_2) = (n_1 \alpha(h_1)(n_2), h_1 h_2)$ .

Notation:  $N \rtimes H$  or  $N \rtimes_\alpha H$ , if  $\alpha$  is not clear from context.


Prop. With notation as above,

- (1)  $N \rtimes H$  is a group.
- (2)  $\exists$  a split exact sequence  $1 \rightarrow N \rightarrow N \rtimes H \xrightarrow{\pi} H \rightarrow 1$   
(and thus  $N$  is a normal subgroup of  $N \rtimes H$ ).

Pf/ HW.  $\square$

Prop. Given any split exact sequence  $1 \rightarrow N \rightarrow G \xrightarrow{\pi} H \rightarrow 1$ ,  
we have seen there is a natural mapping  $\alpha: H \rightarrow \text{Aut}(N)$  given,  
roughly, by conjugation by elements of  $H$ . Then  $G \cong N \rtimes_{\alpha} H$ .

Pf/ HW.  $\square$

Example There are 2 homomorphisms  $\alpha: \mathbb{Z}_2 \rightarrow \text{Aut}(\mathbb{Z}_4) = \{id_{\mathbb{Z}_4}, \gamma_3\} \cong \mathbb{Z}_2$   


(1)  $\alpha(0) = \alpha(1) = id_{\mathbb{Z}_4} : 1 \mapsto 1$ . In this case  $\mathbb{Z}_2 \rtimes_{\alpha} \mathbb{Z}_4 = \mathbb{Z}_2 \times \mathbb{Z}_4$ .

(2)  $\alpha(0) = id_{\mathbb{Z}_4}$ ,  $\alpha(1) = \gamma_3$ . In this case,  $\mathbb{Z}_2 \rtimes_{\alpha} \mathbb{Z}_4 \cong D_4$

## Wreath Products

Def. Let  $P < S_n$ , and let  $G$  be a group. The wreath product of  $G$  with  $P$  is

$$G \wr P_n := G^{x_n} \rtimes P$$

where  $P \rightarrow \text{Aut}(G^{x_n})$  by permuting the components of  $G^{x_n}$ , i.e. for  $\sigma \in P$ ,  $\sigma(g_1, \dots, g_n) = (g_{\sigma(1)}, \dots, g_{\sigma(n)})$ . Thus,

$$(g_1, \dots, g_n, \sigma)(g'_1, \dots, g'_n, \tau) = (g_1 g'_{\sigma(1)}, \dots, g_n g'_{\sigma(n)}, \sigma\tau).$$


---

One way of thinking about  $G \wr P$  is to identify  $P$  with a group of  $n \times n$  permutation matrices. If  $M \in P$ , then wherever there is an entry of 1 in  $M$ , replace it by some element of  $G$ . This gives an  $n \times n$  matrix with whose nonzero entries that are elements of  $G$ . Multiply two such matrices in the natural way. (See the example, below.)

Example Let  $G = \mathbb{Z}$  and let  $P = \langle (123) \rangle \leq S_3$ .

⑥

We think of  $P$  as the set of permutation matrices  $\left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \right\}$ .

Elements of  $\mathbb{Z} \rtimes P$  have the form

$$\begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix}, \begin{bmatrix} 0 & 0 & a' \\ b' & 0 & 0 \\ 0 & c' & 0 \end{bmatrix}, \begin{bmatrix} 0 & a'' & 0 \\ 0 & 0 & b'' \\ c'' & 0 & 0 \end{bmatrix} \quad \text{where } a, b, c, a', b', c', a'', b'', c'' \in \mathbb{Z}.$$

For example,  $\begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 5 \\ 3 & 0 & 0 \\ 0 & 9 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 7 \\ 4 & 0 & 0 \\ 0 & 9 & 0 \end{bmatrix}$

note that  $0+9=9$

Def. Let  $N, H$  be groups. Then  $N \rtimes H := N \rtimes P(H)$  where  $P(H)$  is the group  $H$ , thought of as a permutation group via Cayley ( $H$  acts on itself via left multiplication, and left multiplication permutes the elements of  $H$ ).

## The Jordan-Hölder Theorem

7

Let  $G$  be a finite group. A **composition series** for  $G$  is a maximal chain of subgroups

$$1 = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_{n-1} \triangleleft H_n = G$$

"Maximal" means that one could not refine the chain by adding more subgroups, i.e. for each  $i$ , if  $\exists \tilde{H}$  s.t.  $H_i \triangleleft \tilde{H} \triangleleft H_{i+1}$ , then  $\tilde{H} = H_i$  or  $\tilde{H} = H_{i+1}$ .

The **factors** of a composition series are the groups  $H_{i+1}/H_i$ . (Maximality implies the factors are simple groups.) The **length** of the composition series is  $n$ .

**Thm.** (Jordan-Hölder) The length and the list of composition factors (up to a permutation of the list) is independent of  $G$ .

Example Let  $C_n$  be the cyclic group of order  $n$

8

Composition Series

$$C_1 \triangleleft C_2 \triangleleft C_4 \triangleleft C_{12}$$

$$C_1 \triangleleft C_2 \triangleleft C_6 \triangleleft C_{12}$$

$$C_1 \triangleleft C_3 \triangleleft C_6 \triangleleft C_{12}$$

Composition factors

$$C_2, C_2, C_3$$

$$C_2, C_3, C_2$$

$$C_3, C_2, C_2$$

length

3

3

3