the kernel. We have

$$\begin{aligned}\phi(a) = L_a = \mathrm{id} &\Leftrightarrow agH = gH \text{ for all } g \in G\\ &\Leftrightarrow g^{-1}agH = H \text{ for all } g \in G\\ &\Leftrightarrow g^{-1}ag \in H \text{ for all } g \in G\\ &\Leftrightarrow a \in gHg^{-1} \text{ for all } g \in G.\end{aligned}$$

Therefore the kernel is $\bigcap_{g\in G} H^{g^{-1}} = \bigcap_{a\in G} H^a = H_G$. By the 1st Isomorphism Theorem we have that $H_G \trianglelefteq G$ and

$$G/H_G = G/\ker\phi \cong \mathrm{im}\,\phi$$

where $\mathrm{im}\,\phi \leq \mathrm{Sym}\,(X)$. As $|X| = n$ we have that $\mathrm{Sym}\,(X) \cong S_n$ and thus $G/H_G$ isomorphic to a subgroup of $S_n$. □.

**Corollary 5.11** *(Poincaré's Lemma). Let G be a finite simple group with a subgroup H such that $[G : H] = n > 1$. Then*

$$G \cong K$$

*for some $K \leq S_n$. In particular $|G|$ divides $|S_n| = n!$.*

**Proof** $H_G$ is a normal subgroup of $G$ and as $H_G$ is contained in $H$ we can't have $H_G = G$. Now $G$ is simple and we conclude that $H_G = \{1\}$. The result now follows from Theorem 5.11 as $G/\{1\} \cong G$. □

**Example 5**. Let us give another proof of the fact that there is no simple group of order 12. We argue by contradiction and suppose that $G$ is a simple groups with 12 elements. By the Sylow theorems we have a subgroup of order 4 and thus of index 3. By Corollary 5.12 if follows that $12 = |G|$ divides the $3! = 6$. This is absurd.

We end this section by proving the 3rd Sylow Theorem. We need first some preliminary work.

**Definition** Let $H \leq G$. The *normalizer* of $H$ in $G$ is

$$N_G(H) = \{g \in G : \ H^g = H\}.$$

One can easily check that this is a subgroup of $G$ (in fact it follows also from next remark as $N_G(H)$ turns out to be a stabiliser with respect to a certain $G$-action) and clearly $H \trianglelefteq N_G(H)$.

**Remarks**. (1) Let $X$ be the set of all subgroups of $G$. As we have seen before $G$ acts naturally on $X$ by conjugation and so we can think of $X$ as a $G$-set with respect to this action. The stabilizer of the subgroup $H$ is then $N_G(H)$ and the Orbit-Stabilizer theorem tells us that the number of conjugates of $H$, that is the size of the $G$ orbit $\{H^g : g \in G\}$, is $[G : N_G(H)]$.

(2) Let $P$ be a Sylow p-subgroup of $G$. By the 2nd Sylow Theorem, we know that the Sylow $p$-subgroups form a single conjugacy class $\{P^g : g \in G\}$. By Remark (1) the total number of all Sylow $p$-subgroups is then $n(p) = [G : N_G(P)]$.

**Lemma 5.12** *Let $P$ be a Sylow $p$-subgroup of $G$. Then $P$ is the unique Sylow $p$-subgroup of $N_G(P)$.*

**Proof** Let $Q$ be any Sylow $p$-subgroup of $N_G(P)$. By the second Sylow Theorem we have

$$Q = P^a$$

for some $a \in N_G(P)$. But then $Q = P^a = P$ since $a$ normalizes $P$. $\Box$.

**Proof of the 3rd Sylow Theorem**. Let $P$ be a Sylow $p$-subgroup of $G$. Since the Sylow $p$-subgroups form a single conjugacy class

$$\{P^a : \ a \in G\},$$

we know from the remark above that their number is

$$n(p) = [G : N_G(P)].$$

In particular $n(p)$ divides $|G|$. This proves (ii). To prove (i) we need more work. Let $N = N_G(P)$ and let $X$ be the collection of all the right $N$ cosets of $G$ that we consider as a $P$-set. Write $X$ as a disjoint union of $P$-orbits, say

$$X = Na_1 * P \cup Na_2 * P \cup \cdots \cup Na_m * P$$

where we assume that the first orbit $Na_1 * P$ is the one containing the coset $N \cdot 1 = N$ and we can also then assume that $a_1 = 1$ From this we get that

$$\begin{aligned} n(p) &= |Na_1 * P| + |Na_2 * P| + \cdots + |Na_m * P| \\ &= [P : P \cap N^{a_1}] + [P : P \cap N^{a_2}] + \cdots + [P : P \cap N^{a_m}]. \end{aligned}$$

Now notice that $P \cap N^{a_i} = P$ iff $P \leq N^{a_i}$ iff $P^{a_i^{-1}} \leq N$. However, by Lemma 5.9, this happens iff $P^{a_i^{-1}} = P$ that happens iff $a_i \in N_G(P)$. But then $Na = Na_i \in Na_i * P$ and as the only orbit containing $N$ is $Na_1 * P$, it follows that $i = 1$. (Notice also that $a_1 \in N_G P$ and thus $[P : P \cap N^{a_1}] = 1$). We conclude from this that $[P : P \cap N^{a_i}]$ is divisble by $p$ for $i = 2, \ldots, m$ and that $[P : P \cap N^{a_1}] = 1$. Hence $n(p) = 1 + pr$ for some non-negative integer $r$. $\Box$

# 6 Semidirect products and groups of order $\leq 15$

## I. Semidirect products.

We will now introduce a generalization of direct products that is very useful for describing and constructing groups. As with direct products these come in two disguises internal and external semidirect products.

**Notation**. Suppose that $N$ is a group and $\phi : N \to N$ is an automorphism. In this section we will use $b^\phi$ for the value of $b$ under $\phi$ (instead of $\phi(b)$). This will actually make things look clearer. We will also operate a composition of two automorphisms from left to right. Thus

$$b^{\psi\circ\phi} = (b^\psi)^\phi.$$

**Definition**. Let $G$ be a group and $N \trianglelefteq G, H \leq G$. We say that $G$ is the *internal semidirect product* of $N$ by $H$ if $G = HN$ and $H \cap N = \{1\}$.

**Remark**. The definition is thus very similar to the definition of an internal direct product. The only differenct is that one of the groups $H$ does not have to be normal in general. When $H$ is normal as well then we get a direct product.

**Lemma 6.1** *Let $G$ be an internal semidirect product of $N$ by $H$, then the following hold.*

*(1) Every element $g \in G$ can be written uniquely as $g = ab$ with $a \in H$ and $b \in N$.*

*(2) Let $a_1, a_2 \in H$ and $b_1, b_2 \in N$. Then*

$$(a_1b_1) \cdot (a_2b_2) = (a_1a_2) \cdot (b_1^{a_2}b_2)$$

**Proof** (1) If $a_1b_1 = a_2b_2$ then $a_2^{-1}a_1 = b_2b_1^{-1}$ is in $H \cap N$ and thus trivial. So $a_1 = a_2$ and $b_1 = b_2$).

(2) We have

$$(a_1b_1) \cdot (a_2b_2) = (a_1a_2) \cdot (a_2^{-1}b_1a_2b_2) = (a_1a_2) \cdot (b_1^{a_2}b_2).$$

This finishes the proof. □

**Remark**. Thus, like for internal direct products, we can treat elements like pairs $ab$ where $a$ is the $H$ component and $b$ is the $N$ component. Furthermore multiplying two such elements $a_1b_1$ and $a_2b_2$ gives us a new element whose $H$ compenent is $a_1a_2$ and whose

$N$ component is $b_1^{a_2}b_2$. It follows that if we know the structure of $H$ and $N$ and if we know how $H$ acts on $N$ by conjugation, then we know the structure of the semidirect product $G$. If you for example had a multiplication table for $H$ and $N$ and you knew how $H$ acts on $N$ by conjugation then you could write down a multiplication table for $G$.

**Remark**. For $a \in H$, let $\phi_a : N \to N$ be the conjugation by $a$. We have seen previously that this map is an automorphism. Now

$$x^{\phi_{ab}} = x^{ab} = (x^a)^b = (x^{\phi_a})^{\phi_b} = x^{\phi_a \circ \phi_b}.$$

Consider the map $\Psi : H \to \mathrm{Aut}\,(N)$, $a \mapsto \phi_a$. As $\Psi(ab) = \phi_{ab} = \phi_a \circ \phi_b = \Psi(a) \circ \Psi(b)$, this map is a homomorphism. Notice also

$$a_1b_1 \cdot a_2b_2 = (a_1a_2) \cdot (b_1^{a_2}b_2) = (a_1a_2) \cdot (b_1^{\phi_{a_2}}b_2) = (a_1a_2) \cdot (b_1^{\Psi(a_2)}b_2)$$

This motivates the following structure.

**Definition** Let $N, H$ be groups and let $\Psi : H \to \mathrm{Aut}\,(N)$ be a homomorphism. The external semidirect product $H \ltimes_\Psi N$, of $N$ by $H$ with respect to $\Psi$, is the cartesian set product of $H$ and $N$ with the binary operation

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2, b_1^{\Psi(a_2)}b_2)$$

$H \ltimes_\Psi N$ **is a group**. First let us check the associativity. Firstly

$$\begin{aligned} [(a_1, b_1) \cdot (a_2, b_2)] \cdot (a_3, b_3) &= (a_1a_2, b_1^{\Psi(a_2)}b_2) \cdot (a_3, b_3) \\ &= (a_1a_2a_3, (b_1^{\Psi(a_2)}b_2)^{\Psi(a_3)}b_3) \end{aligned}$$

Since $\Psi(a_3) \in \mathrm{Aut}\,(N)$ and since $\Psi$ is a homorphism, we get

$$\begin{aligned} (b_1^{\Psi(a_2)}b_2)^{\Psi(a_3)}b_3 &= b_1^{\Psi(a_2)\Psi(a_3)}b_2^{\Psi(a_3)}b_3 \\ &= b_1^{\Psi(a_2a_3)}b_2^{\Psi(a_3)}b_3. \end{aligned}$$

Then secondly

$$\begin{aligned} (a_1, b_1) \cdot [(a_2, b_2) \cdot (a_3, b_3)] &= (a_1, b_1) \cdot (a_2a_3, b_2^{\Psi(a_3)}b_3) \\ &= (a_1a_2a_3, b_1^{\Psi(a_2a_3)}b_2^{\Psi(a_3)}b_3). \end{aligned}$$

This shows that the associative law holds. To see that $(1, 1)$ is the identity. Notice that any automorphism maps 1 to itself and that $\Psi(1) = \mathrm{id}$. Thus

$$(1, 1) \cdot (a, b) = (1 \cdot a, 1^{\Psi(a)}b) = (a, b)$$

and

$$(a, b) \cdot (1, 1) = (a \cdot 1, b^{\Psi(1)} \cdot 1) = (a, b^{\mathrm{id}} \cdot 1) = (a, b).$$

Finally, the inverse of $(a, b)$ is $(a^{-1}, (b^{\Psi(a^{-1})})^{-1})$ since

$$(a, b) \cdot (a^{-1}, (b^{\Psi(a^{-1})})^{-1}) = (a \cdot a^{-1}, b^{\Psi(a^{-1})}(b^{\Psi(a^{-1})})^{-1}) = (1, 1)$$

and

$$\begin{aligned}(a^{-1},(b^{\Psi(a^{-1})})^{-1})\cdot(a,b) &= (aa^{-1},((b^{\Psi(a^{-1})})^{-1})^{\Psi(a)}b)\\ &= (1,(b^{\Psi(a^{-1})\Psi(a)})^{-1}b)\\ &= (1,(b^{\Psi(1)})^{-1}b)\\ &= (1,(b^{\text{id}})^{-1}b)\\ &= (1,1).\end{aligned}$$

**Remark**. Consider an internal semidirect product of $N$ by $H$ and let $\Psi : H \rightarrow \text{Aut}\,(N)$ be the homomorphism that maps $a$ to $\phi_a$ where the latter is the automorphism that takes $b$ to $b^a$. Using the data $N, H$ and $\Psi$, we can also construct the external semidirect product $H \ltimes_{\Psi} N$. Not surprisingly, the two are isomorphic (see Exercise 1 on Sheet 10).

## II. Groups of order less than 16.

In this section (and on the exercise sheets) we play with our new tools and find all groups of order up to and including 15. We have already shown previously (Exercise 2 on sheet 9) that the only group of order 15 is $\mathbb{Z}_{15}$ and we have no difficulty with groups of order 1. When $p$ is a prime, there is exactly one group of order $p$, the cyclic group $\mathbb{Z}_p$ of order $p$. On exercise sheet 8 we also show that there are only two groups of order $p^2$, namely $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \oplus \mathbb{Z}_p$.

**Semidirect products of cyclic groups**. Suppose that $G = HN$ is an internal semidirect product of a cyclic group $N = \langle a \rangle$ by another cyclic group $\langle b \rangle$. We have that

$$a^b = a^r \tag{5}$$

for some $r \in \mathbb{Z}$. Inductively it follows that $a^{b^n} = a^{r^n}$ and then that $(a^m)^{b^n} = (a^{b^n})^m = a^{mr^n}$. Thus the structure of $G$ is determined by (5) and the orders of $a$ and $b$.

We will now introduce an infinite family of groups, many of which will crop up in the list of groups of orders 1 to 15.

**Example.**($D_{2n}$, the dihedral group of order $2n$). Consider a regular $n$-gon in the complex plane with corners $1, u, u^2, \ldots, u^{n-1}$ where $u = e^{2\pi i/n}$ (draw a figure). The symmetry group of this regular $n$-gon is generated by a counter clockwise rotation $a$ of $2\pi/n$ around the origin and the reflection $b$ in the real axis. This can be described explicitly as follows:

$$\begin{aligned}a(z) &= e^{2\pi i/n}\cdot z\\ b(z) &= \bar{z}.\end{aligned}$$

Let us calculate

$$\begin{aligned}b^{-1}ab(z) &= bab(z)\\ &= ba(\bar{z})\\ &= b(e^{2\pi i/n}\cdot\bar{z})\\ &= e^{-2\pi i/n}z\\ &= a^{-1}(z).\end{aligned}$$

This means that the symmetry group is a group of order $2n$ that is a semidirect product of $\langle a\rangle$, a cyclic group of order $n$, and $\langle b\rangle$, a cyclic group of order 2. Furthermore the action of $\langle b\rangle$ on $\langle a\rangle$ is determined by $a^b = a^{-1}$. The unique group of order $2n$ with a normal cyclic subgroup $\langle a\rangle$ of order $n$, and a cyclic subgroup $\langle b\rangle$ where $a^b = a^{-1}$ is called the dihedral group of order $2n$ and is denoted $D_{2n}$.

**Theorem 6.2** *Let $p$ be an odd prime. There are (up to isomorphism) exactly two groups of order $2p$ these are*

$$\mathbb{Z}_{2p} \ \ \textit{and} \ \ D_{2p}.$$

**Proof** By the Sylow theorems (or Cauchy's thm) there is a subgroup $N = \langle a\rangle$ of order $p$. Since $N$ is of index 2 it is normal. There is also a group $H = \langle b\rangle$ of order 2. Clearly $H \cap N = \{1\}$, since it is a subgroup of both $H$ and $N$ and thus its order divides both 2 and $p$. So we have that $G$ is a semidirect product of $N$ by $H$. To determine the group structure it remains to see how $H$ can act on $N$. Now

$$b^{-1}ab = a^r$$

for some $0 \le r \le p-1$. Using the fact that $b$ is of order 2, we see that

$$a = b^{-1}(b^{-1}ab)b = b^{-1}a^rb = (b^{-1}ab)^r = a^{r^2}.$$

This implies that $a^{r^2-1} = 1$ and thus $p$ must divide $r^2-1 = (r-1)(r+1)$. The only possibilities for this to happen is when $r = 1$ or $r = p-1$. In the first case the group is abelian and $G = \langle ba\rangle$ is a cyclic group of order $2p$. (Notice that $(ba)^2 = a^2 \neq 1$ and $(ba)^p = b \neq 1$ so the order of $ba$ is $2p$ by Lagrange's theorem). In the latter case we have the relations

$$a^p = 1, \ \ b^2 = 1, \ \ bab^{-1} = a^{p-1} = a^{-1}$$

which gives us $D_{2p}$ as we have seen. □

**Remark**. The only orders up to 15 that are not covered by 1, 15, $p$, $p^2$ and $2p$ are 8 and 12. These are dealt with on the excercise sheets 9 and 10.

We end by constructing a certain group of order 12, using the external semidirect product.

**Example**. Let $N = \langle a\rangle$ be a cyclic group of order 3 and $H = \langle b\rangle$ be a cyclic group of order 4. The map

$$\phi : N \to N, \, x \mapsto x^{-1}$$

is in $\mathrm{Aut}\,(N)$. The map

$$\Psi : H \to \mathrm{Aut}\,(N), \ b^r \mapsto \phi^r$$

is a homomorphism. It is well defined as $b^r = b^s \Rightarrow b^{s-r} = 1 \Rightarrow 4|(r-s) \Rightarrow \phi^{s-r} = \mathrm{id} \Rightarrow \phi^r = \phi^s$. Consider the external semidirect product $T = H \ltimes_\Psi N$. It is a group of order 12 with a cyclic normal Sylow 3-subgroup of order 3 and a cyclic Sylow 2-subgroup of order 4.

From our study in this chapter and the exercise sheets we can conclude that the groups of order $\le 15$ are (up to isomorphism)

| order | groups |
|---|---|
| 1 | $\{1\}$ |
| 2 | $\mathbb{Z}_2$ |
| 3 | $\mathbb{Z}_3$ |
| 4 | $\mathbb{Z}_4,\ \mathbb{Z}_2 \oplus \mathbb{Z}_2$ |
| 5 | $\mathbb{Z}_5$ |
| 6 | $\mathbb{Z}_6,\ D_6$ |
| 7 | $\mathbb{Z}_7$ |
| 8 | $\mathbb{Z}_8,\ \mathbb{Z}_4 \oplus \mathbb{Z}_2,\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2,\ D_8,\ Q$ |
| 9 | $\mathbb{Z}_9,\ \mathbb{Z}_3 \oplus \mathbb{Z}_3$ |
| 10 | $\mathbb{Z}_{10},\ D_{10}$ |
| 11 | $\mathbb{Z}_{11}$ |
| 12 | $\mathbb{Z}_4 \oplus \mathbb{Z}_3,\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3,\ A_4,\ D_{12},\ T$ |
| 13 | $\mathbb{Z}_{13}$ |
| 14 | $\mathbb{Z}_{14},\ D_{14}$ |
| 15 | $\mathbb{Z}_{15}$ |