Chapter 6

Soluble Groups

We have already met the concept of a composition series for a group. In this chapter we shall consider groups whose composition factors are all abelian. Think of this as the class of groups that can be built using only abelian groups.

6.1 Definition of soluble groups

Definition 6.1 Let G be a group and $x, y \in G$. The *commutator* of x and y is the element

$$[x, y] = x^{-1}y^{-1}xy.$$

Note that the following equations hold immediately:

$$\begin{aligned} [x, y] &= x^{-1}x^y \\ [x, y] &= (y^{-1})^x y \\ xy &= yx[x, y]. \end{aligned} \tag{6.1}$$

The latter tells us that the commutator essentially measures by how much x and y fail to commute.

Lemma 6.2 *Let G and H be groups, let $\phi\colon G \to H$ be a homomorphism and let $x, y, z \in G$. Then*

(i) $[x, y]^{-1} = [y, x]$;

(ii) $[x, y]\phi = [x\phi, y\phi]$;

(iii) $[x, yz] = [x, z]\,[x, y]^z$;

(iv) $[xy, z] = [x, z]^y\,[y, z]$.

PROOF: (i) $[x,y]^{-1} = (x^{-1}y^{-1}xy)^{-1} = y^{-1}x^{-1}yx = [y,x]$.

(ii) $[x,y]\phi = (x^{-1}y^{-1}xy)\phi = (x\phi)^{-1}(y\phi)^{-1}(x\phi)(y\phi) = [x\phi, y\phi]$.

(iii) For this and part (iv), we shall rely on Equation (6.1) and view it as telling us how to exchange group elements at the expense of introducing commutators. (This is known as 'collection'.) So

$$xyz = yzx[x,yz]$$

but if we collect one term at a time we obtain

$$\begin{aligned} xyz &= yx[x,y]z \\ &= yxz[x,y]^z \\ &= yzx[x,z]\,[x,y]^z. \end{aligned}$$

Hence

$$yzx[x,yz] = yzx[x,z]\,[x,y]^z,$$

so

$$[x,yz] = [x,z]\,[x,y]^z.$$

(iv)

$$xyz = zxy[xy,z]$$

and

$$\begin{aligned} xyz &= xzy[y,z] \\ &= zx[x,z]y[y,z] \\ &= zxy[x,z]^y[y,z]. \end{aligned}$$

Comparing we deduce

$$[xy,z] = [x,z]^y[y,z].$$

□

Both parts (iii) and (iv) can be proved by a more simple-minded expansion of the terms on both sides, but more can be learnt and understood via the collection process.

Definition 6.3 Let G be a group. The *derived subgroup* (or *commutator subgroup*) G' of G is the subgroup generated by all commutators of elements from G:

$$G' = \langle\, [x,y] \mid x,y \in G \,\rangle.$$

Part (i) of Lemma 6.2 tells us that the inverse of a commutator is again a commutator, but we have no information about products of commutators. Consequently, a typical element of G' has the form

$$[x_1,y_1]\,[x_2,y_2]\ldots[x_n,y_n]$$

where $x_i, y_i \in G$ for each i.

Example 6.4 (i) In an abelian group G

$$[x, y] = x^{-1}y^{-1}xy = 1 \qquad \text{for all } x \text{ and } y,$$

so $G' = \mathbf{1}$. (The condition $G' = \mathbf{1}$ is equivalent to G being abelian.)

(ii) Let's calculate the derived group of Q_8. Note that -1 is central in Q_8, so we only need to calculate the commutators of i, j and k.

$$[i, j] = (-i)(-j)ij = ij(ij) = (ij)k = k^2 = -1$$
$$[i, k] = (-i)(-k)ik = i(ki)k = i(jk) = i^2 = -1$$
$$[j, k] = (-j)(-k)jk = jk(jk) = (jk)i = i^2 = -1$$

So $Q_8' = \langle -1 \rangle$.

Definition 6.5 The *derived series* $(G^{(i)})$ (for $i \geqslant 0$) is the chain of subgroups of the group G defined by

$$G^{(0)} = G$$

and

$$G^{(i+1)} = (G^{(i)})' \qquad \text{for } i \geqslant 0.$$

So $G^{(1)} = G'$, $G^{(2)} = (G')' = G''$, etc. We then have a chain of subgroups

$$G = G^{(0)} \geqslant G^{(1)} \geqslant G^{(2)} \geqslant \cdots .$$

We shall see later that this is indeed a series in the sense of Definition 4.1 (in that each term is normal in the previous).

Definition 6.6 A group G is *soluble* (*solvable* in the U.S.) if $G^{(d)} = \mathbf{1}$ for some d. The least such d is the *derived length* of G.

Since when forming the derived series, we take the derived subgroup of the previous term at each stage, once we have a repetition then the series becomes constant. Thus if G is a soluble group of derived length d, its derived series has the form

$$G = G^{(0)} > G^{(1)} > G^{(2)} > \cdots > G^{(d)} = \mathbf{1}.$$

Example 6.7 Looking back at Example 6.4 we see that:

(i) Any abelian group is soluble with derived length 1.

(ii) The group Q_8 is soluble with derived length 2.

We seek to understand the properties of soluble groups, and to produce equivalent formulations so that examples can be more easily described. Accordingly, we begin by establishing basic properties of the derived subgroup and the derived series.

Lemma 6.8 (i) *If H is a subgroup of G, then $H' \leqslant G'$.*

(ii) *If $\phi\colon G \to K$ is a homomorphism, then $G'\phi \leqslant K'$.*

(iii) *If $\phi\colon G \to K$ is a surjective homomorphism, then $G'\phi = K'$.*

PROOF: (i) If $x, y \in H$, then $[x, y]$ is a commutator of elements of G so belongs to the derived subgroup of G:

$$[x, y] \in G' \qquad \text{for all } x, y \in H.$$

Therefore

$$\langle\, [x, y] \mid x, y \in H \,\rangle \leqslant G',$$

so $H' \leqslant G'$.

(ii) If $x, y \in G$, then $[x, y]\phi = [x\phi, y\phi] \in K'$. Since K' is closed under products, it follows that any product of commutators in G is mapped into K' by ϕ. Thus $G'\phi \leqslant K'$.

(iii) Let $a, b \in K$. Since ϕ is surjective, there exists $x, y \in G$ such that $a = x\phi$ and $b = y\phi$. Thus

$$[a, b] = [x\phi, y\phi] = [x, y]\phi \in G'\phi.$$

Thus

$$[a, b] \in G'\phi \qquad \text{for all } a, b \in K.$$

This forces $K' \leqslant G'\phi$. Using (ii) gives $K' = G'\phi$, as required. □

Lemma 6.9 *Subgroups of soluble groups are soluble.*

PROOF: Let G be a soluble group and H be a subgroup of G. We start by claiming that $H^{(i)} \leqslant G^{(i)}$ for all i. We will prove the claim by induction on i. The case $i = 0$ is the inclusion $H \leqslant G$ which holds by assumption.

Now suppose $H^{(i)} \leqslant G^{(i)}$. Apply Lemma 6.8(i) to give

$$(H^{(i)})' \leqslant (G^{(i)})';$$

that is,

$$H^{(i+1)} \leqslant G^{(i+1)}.$$

This completes the induction.

Now since G is soluble, $G^{(d)} = \mathbf{1}$ for some d. Therefore, as $H^{(d)} \leqslant G^{(d)}$, we have $H^{(d)} = \mathbf{1}$ and so we deduce that H is soluble. □

Lemma 6.10 *Homomorphic images of soluble groups are soluble.*

PROOF: Let G be a soluble group, and let K be a homomorphic image of G. Thus there exists a surjective homomorphism $\phi\colon G \to K$. We claim that $K^{(i)} = G^{(i)}\phi$ for all i. We will prove the claim by induction on i. The case $i = 0$ is the equation $K = G\phi$ which holds by assumption.

Now suppose $K^{(i)} = G^{(i)}\phi$. Thus ϕ induces a surjective homomorphism $G^{(i)} \to K^{(i)}$ and Lemma 6.8(iii) gives

$$(K^{(i)})' = (G^{(i)})'\phi;$$

that is,

$$K^{(i+1)} = G^{(i+1)}\phi.$$

This completes the induction.

Now as G is soluble, $G^{(d)} = \mathbf{1}$ and thus

$$K^{(d)} = G^{(d)}\phi = \mathbf{1}\phi = \mathbf{1}.$$

Hence K is soluble. □

It follows that quotient groups (which are the same as homomorphic images) of soluble groups are themselves soluble. There is a rather strong converse to the above lemma:

Proposition 6.11 *Let G be a group and N be a normal subgroup of G such that both G/N and N are soluble. Then G is soluble.*

PROOF: Let $\pi\colon G \to G/N$ be the natural map. By assumption $(G/N)^{(d)} = \mathbf{1}$ and $N^{(e)} = \mathbf{1}$ for some d and e. Now, by Lemma 6.10,

$$G^{(d)}\pi = (G/N)^{(d)} = \mathbf{1}.$$

Hence

$$G^{(d)} \leqslant \ker\pi = N.$$

Therefore, by Lemma 6.9,

$$(G^{(d)})^{(e)} \leqslant N^{(e)} = \mathbf{1};$$

that is,

$$G^{(d+e)} = \mathbf{1}.$$

Thus G is soluble. □

Note It is not necessarily the case that G has derived length $d + e$: this is just an upper bound. For example, if G is the direct product of N and G/N then one can show that the derived length of G is the *maximum* of d and e.

We have observed that if $\phi\colon G \to K$ is a surjective homomorphism then $G'\phi = K'$. In particular, if ϕ is an automorphism of G (that is, an isomorphism $G \to G$), then $G'\phi = G'$. We give the following special name to subgroups satisfying this property.

Definition 6.12 A subgroup H of a group G is said to be a *characteristic subgroup* of G if $x\phi \in H$ for all $x \in H$ and all automorphisms ϕ of G. We write

$$H \operatorname{char} G$$

to indicate that H is a characteristic subgroup of G.

The definition requires that $H\phi \leqslant H$ for all automorphisms ϕ of G. But then $H\phi^{-1} \leqslant H$, and applying ϕ yields $H \leqslant H\phi$. Thus H is a characteristic subgroup if and only if $H\phi = H$ for all automorphisms ϕ of G.

Example 6.13 (i) The trivial subgroup $\mathbf{1}$ is fixed by all automorphisms of G, and hence is characteristic in G.

(ii) The group G is a characteristic subgroup of itself, since all automorphisms are bijections.

(iii) Consider the group S_5. The only normal subgroups of S_5 are $\mathbf{1}$, A_5, and S_5. Since A_5 is the only normal subgroup of S_5 of order 60, it must be fixed by all automorphisms of S_5, so $A_5 \operatorname{char} S_5$.

(iv) Let $G = C_{15} = C_3 \times C_5$. Then the subgroup of order 3 in G contains *all* elements of order 3 in G, and hence must be mapped to itself by all automorphisms of G. The same applies to the subgroup of order 5. Thus both C_3 and C_5 are characteristic subgroups of G.

(v) Consider the group $V_4 = \{1, a, b, c\}$. This has three proper nontrivial normal subgroups, all of order 2, generated by a, b and c respectively. The permutation $(a\ b\ c)$ is an automorphism of V_4. Hence, no proper nontrivial normal subgroup of V_4 is fixed by all automorphisms of V_4, and hence the only characteristic subgroups of V_4 are $\mathbf{1}$ and V_4.

Our observation above then is that

$$G' \operatorname{char} G$$

for all groups G and we shall soon see that all terms in the derived series are also characteristic.

Lemma 6.14 *Let G be a group.*

(i) *If $H \operatorname{char} G$, then $H \trianglelefteqslant G$.*

(ii) *If $K \operatorname{char} H$ and $H \operatorname{char} G$, then $K \operatorname{char} G$.*

(iii) *If $K \operatorname{char} H$ and $H \trianglelefteqslant G$, then $K \trianglelefteqslant G$.*

Thus there is considerable difference between characteristic subgroups and normal subgroups. For example, note that in general

- $K \trianglelefteqslant H \trianglelefteqslant G$ does not imply $K \trianglelefteqslant G$.
- If $\phi\colon G \to K$ is a homomorphism and $H \operatorname{char} G$, then it does not follow necessarily that $H\phi \operatorname{char} G\phi$. (Consequently the Correspondence Theorem does not work well with characteristic subgroups.)
- If $H \leqslant L \leqslant G$ and $H \operatorname{char} G$, then it does not necessarily follow that $H \operatorname{char} L$.

Proof of Lemma 6.14: (i) If $x \in G$, then $\tau_x\colon g \mapsto g^x$ is an automorphism of G. Hence if $H \operatorname{char} G$, then

$$H^x = H\tau_x = H \qquad \text{for all } x \in G,$$

so $H \trianglelefteqslant G$.

(ii) Let ϕ be an automorphism of G. Then $H\phi = H$ (as $H \operatorname{char} G$). Hence the restriction $\phi|_H$ of ϕ to H is an automorphism of H and we deduce

$$x\phi \in K \qquad \text{for all } x \in K$$

(since this is the effect that the restriction $\phi|_H$ has when applied to elements of K). Thus $K \operatorname{char} G$.

(iii) Let $x \in G$. Then $H^x = H$ (as $H \trianglelefteqslant G$) and therefore $\tau_x\colon g \mapsto g^x$ (for $g \in H$) is a bijective homomorphism $H \to H$; that is, τ_x is an automorphism of H. Since $K \operatorname{char} H$, we deduce that $K^x = K\tau_x = K$. Thus $K \trianglelefteqslant G$. □

We have seen that $G' \operatorname{char} G$. Recall the definition of the derived series:

$$G^{(0)} = G, \qquad G^{(i+1)} = (G^{(i)})' \quad \text{for } i \geqslant 0.$$

Therefore

$$G^{(i)} \operatorname{char} G^{(i-1)} \operatorname{char} G^{(i-2)} \operatorname{char} \cdots \operatorname{char} G^{(1)} \operatorname{char} G^{(0)} = G.$$

Applying Lemma 6.14(ii) we see that each $G^{(i)}$ is a characteristic subgroup (and hence a normal subgroup) of G for each i.

Proposition 6.15 *The derived series*

$$G = G^{(0)} \geqslant G^{(1)} \geqslant G^{(2)} \geqslant \cdots$$

is a chain of subgroups, each of which is a characteristic subgroup of G, and hence each of which is a normal subgroup of G. □

In particular, if G is a soluble group of derived length d then

$$G = G^{(0)} > G^{(1)} > \cdots > G^{(d)} = \mathbf{1}$$

and this is a normal series (each term is normal in G). In particular, we can consider the factors

$$G^{(0)}/G^{(1)},\ G^{(1)}/G^{(2)}, \ldots, G^{(d-1)}/G^{(d)};$$

i.e., the quotient groups $G^{(i)}/(G^{(i)})'$ for $i = 0, 1, \ldots, d-1$.

We now deduce some information about these factors.

Lemma 6.16 *Let G be a group and N be a normal subgroup of G. Then G/N is abelian if and only if $G' \leqslant N$.*

In particular, G/G' is an abelian group and it is the largest quotient group of G which is abelian. We often call G/G' the *abelianisation* of G.

PROOF: Suppose G/N is abelian. Then

$$Nx \cdot Ny = Ny \cdot Nx \qquad \text{for all } x, y \in G,$$

so

$$N[x, y] = (Nx)^{-1}(Ny)^{-1}(Nx)(Ny) = N1 \qquad \text{for all } x, y \in G.$$

Thus $[x, y] \in N$ for all $x, y \in G$ and we obtain $G' \leqslant N$.

Conversely if $G' \leqslant N$, then $[x, y] \in N$ for all $x, y \in G$ and reversing the above steps shows that G/N is abelian. □

In particular, the factors occurring in the derived series are all abelian. So if G is a soluble group, then its derived series is a normal series with all factors abelian. The following result strengthens this.

Theorem 6.17 *Let G be a group. The following conditions are equivalent:*

(i) *G is soluble;*

(ii) *G has a chain of subgroups*

$$G = G_0 \geqslant G_1 \geqslant G_2 \geqslant \cdots \geqslant G_n = \mathbf{1}$$

such that G_i is a normal subgroup of G and G_{i-1}/G_i is abelian for $i = 1, 2, \ldots, n$;

(iii) *G has a chain of subgroups*

$$G = G_0 \geqslant G_1 \geqslant G_2 \geqslant \cdots \geqslant G_n = \mathbf{1}$$

such that G_i is a normal subgroup of G_{i-1} and G_{i-1}/G_i is abelian for $i = 1, 2, \ldots, n$.

Condition (ii) says that G has a normal series with abelian factors, while (iii) says that G has a subnormal series with abelian factors.

PROOF: (i) $\Rightarrow$ (ii): The derived series is such a chain of subgroups.
(ii) $\Rightarrow$ (iii): Immediate: If $G_i \trianglelefteq G$ for $G_i \leqslant G_{i-1} \leqslant G$, then $G_i \trianglelefteq G_{i-1}$.
(iii) $\Rightarrow$ (i): Suppose

$$G = G_0 \geqslant G_1 \geqslant G_2 \geqslant \ldots \geqslant G_n = \mathbf{1}$$

is a series where G_{i-1}/G_i is abelian for all i.

Claim: $G^{(i)} \leqslant G_i$ for all i.

We prove the claim by induction on i. Since $G^{(0)} = G = G_0$, the claim holds for $i = 0$.

Suppose $G^{(i)} \leqslant G_i$. Now $G_{i+1} \trianglelefteq G_i$ and G_i/G_{i+1} is abelian. Hence $(G_i)' \leqslant G_{i+1}$ by Lemma 6.16. Further, by Lemma 6.8(i), $(G^{(i)})' \leqslant (G_i)'$. Hence

$$G^{(i+1)} = (G^{(i)})' \leqslant (G_i)' \leqslant G_{i+1}.$$

Hence by induction $G^{(n)} \leqslant G_n = \mathbf{1}$, so $G^{(n)} = \mathbf{1}$ and G is soluble. □

We now have a characterisation that a group is soluble if and only if it has a series with abelian factors. We shall obtain a further such equivalence by linking solubility to composition series.

We saw in Example 6.7 that all abelian groups are soluble. In particular, the infinite cyclic group is soluble, though we know (Example 4.4) that this group does not have a composition series. Accordingly we cannot hope for composition series to give us complete information about soluble groups. It turns out that as long as we avoid the infinite soluble groups, composition series do tell us whether or not our group is soluble.

Theorem 6.18 *Let G be a group. The following conditions are equivalent:*

(i) *G is a finite soluble group;*

(ii) *G has a composition series with all composition factors cyclic of prime order.*

Recall that the abelian simple groups are precisely the cyclic groups of (various) prime orders. Thus part (ii) describes the groups with abelian composition factors.

PROOF: (ii) $\Rightarrow$ (i): Let

$$G = G_0 > G_1 > G_2 > \cdots > G_n = \mathbf{1}$$

be a composition series for G and suppose that all of the factors are cyclic. Then $G_i \trianglelefteqslant G_{i-1}$ and G_{i-1}/G_i is abelian for each i. Thus this is a chain of subgroups as in Theorem 6.17(iii) and therefore G is soluble. Further

$$|G| = |G_0/G_1| \cdot |G_1/G_2| \cdot \ldots \cdot |G_{n-1}/G_n|,$$

a product of finitely many primes, so G is finite.

(i) $\Rightarrow$ (ii): Let G be a finite soluble group. Then by Theorem 6.17, G possesses a chain of subgroups

$$G = G_0 > G_1 > G_2 > \cdots > G_n = \mathbf{1} \tag{6.2}$$

such that $G_i \trianglelefteqslant G_{i-1}$ and G_{i-1}/G_i is abelian for all i. Note that G can only have at most finitely many such series. Thus we may assume that (6.2) is the longest series for G with abelian factors. Such a series must then be a composition series: for if some G_{i-1}/G_i is not simple, then there exists $N \trianglelefteqslant G_{i-1}$ with $G_i < N < G_{i-1}$. We then obtain a series

$$G = G_0 > \cdots > G_{i-1} > N > G_i > \cdots > G_n = \mathbf{1}$$

which is longer than (6.2) and the new factors occurring here satisfy

$$N/G_i \leqslant G_{i-1}/G_i \qquad \text{and} \qquad G_{i-1}/N \cong \frac{G_{i-1}/G_i}{N/G_i}$$

(by the Third Isomorphism Theorem). Since G_{i-1}/G_i is abelian, we see that N/G_i and G_{i-1}/N are abelian. This contradicts the assumption that (6.2) is the longest series with abelian factors.

We now deduce that (6.2) is indeed a composition series and hence the composition factors of G are abelian. Since the only abelian simple groups are cyclic of prime order, we deduce that all the composition factors of G are cyclic of prime order (for various primes). □

Example 6.19 In Example 4.3 we saw that

$$S_4 > A_4 > V_4 > \langle (1\ 2)(3\ 4) \rangle > \mathbf{1}$$

is a composition series for S_4 and the composition factors are C_2, C_3, C_2 and C_2. Hence S_4 is soluble by Theorem 6.18.

Example 6.20 The dihedral group D_{2n} contains an element α of order n, so $\langle \alpha \rangle$ has index 2, and so is normal. Thus

$$D_{2n} > \langle \alpha \rangle > \mathbf{1}$$

is a series for D_{2n} with both factors cyclic. Hence D_{2n} is soluble by Theorem 6.17.

Example 6.21 If $n \geq 5$, then A_n is non-abelian simple group, so is insoluble by Theorem 6.18. As every subgroup of a soluble group is soluble, it follows that S_n is insoluble for $n \geq 5$.

Careful analysis of the examples in Section 3 shows that the groups we considered that were not simple in 3.7–3.10 are also soluble groups.

6.2 Finite soluble groups

For the rest of this chapter we shall work only with finite groups. Our goal is to prove Hall's Theorem on finite soluble groups.

6.2.1 Minimal normal subgroups

In this subsection we will work with finite groups *without* assuming that they are also soluble.

Definition 6.22 Let G be a finite group. A *minimal normal subgroup* of G is a non-trivial normal subgroup of G which properly contains no nontrivial normal subgroups of G.

Thus M is a minimal normal subgroup of G if

(i) $\mathbf{1} < M \trianglelefteqslant G$;

(ii) if $\mathbf{1} \leqslant N \leqslant M$ and $N \trianglelefteqslant G$, then either $N = \mathbf{1}$ or $N = M$.

Note that, apart from the trivial group, all finite groups have minimal normal subgroups. To see this, we start with the group G itself. If this isn't a minimal normal subgroup, then there is a nontrivial subgroup below it which is normal. If this isn't minimal, then there is a nontrivial subgroup below it which is normal in G. Repeating this process must eventually stop (since G is finite) and yield a minimal normal subgroup.

Example 6.23 (i) If $n \geq 5$, then A_n is simple. Thus there are no normal subgroups of S_n contained in A_n, and hence A_n is a minimal normal subgroup of S_n.

(ii) Let $G = A_5 \times A_6$. Then the normal subgroups of G are $\mathbf{1}, A_5, A_6$ and G. Therefore the minimal normal subgroups of G are A_5 and A_6.

Definition 6.24 A non-trivial group G is called *characteristically simple* if the only characteristic subgroups it has are $\mathbf{1}$ and G.

(Recall, from Definition 6.12, that a characteristic subgroup of G is a subgroup which is closed under applying all automorphisms of G.)

Example 6.25 (i) If G is a simple group, then $\mathbf{1}$ and G are the only normal subgroups of G, so G is characteristically simple.

(ii) Recall Example 6.13(v). We proved that V_4 has no characteristic subgroups, so V_4 is characteristially simple.

(iii) If G is nonabelian and soluble, then $G' \operatorname{char} G$ and $1 < G' < G$, so G is not characteristically simple.

The following lemma is easy to prove, but often extremely useful.

Lemma 6.26 *Let G be a group, and let M be a minimal normal subgroup of G. Then M is characteristically simple.*

PROOF: Let K be a characteristic subgroup of M. Then

$$K \operatorname{char} M \trianglelefteqslant G,$$

so $K \trianglelefteqslant G$ by Lemma 6.14(iii). Thus minimality of M forces $K = \mathbf{1}$ or $K = M$. Hence M is indeed characteristically simple. □

Theorem 6.27 *A characteristically simple finite group is a direct product of isomorphic simple groups.*

PROOF: Let G be a finite group which is characteristically simple. Let S be a minimal normal subgroup of G. (So $S \neq \mathbf{1}$. It is possible that $S = G$.) Consider the following set

$$\mathscr{D} = \{\, N \trianglelefteqslant G \mid N = S_1 \times S_2 \times \cdots \times S_k \text{ where each } S_i \text{ is a minimal normal subgroup of } G \text{ isomorphic to } S \,\}.$$

(Recall what we mean by the direct product here: it is an internal direct product, so we need $S_i \cap S_1 \dots S_{i-1} S_{i+1} \dots S_k = \mathbf{1}$ for each i, as well as $N = S_1 S_2 \dots S_k$. We already assume $S_i \trianglelefteqslant G$, so the requirement $S_i \trianglelefteqslant N$ comes for free.)

Note that $S \in \mathscr{D}$, so $\mathscr{D}$ certainly contains non-trivial members. Choose $N \in \mathscr{D}$ of largest possible order. We will prove that $N = G$.

If $N \neq G$ then, as G is characteristically simple, N is not characteristic in G. Hence there exists an automorphism ϕ of G such that

$$N\phi \not\leqslant N.$$

Let $N = S_1 \times S_2 \times \cdots \times S_k$, then there exists i such that

$$S_i\phi \not\leqslant N.$$

Now ϕ is an automorphism of G, so $S_i\phi$ is a minimal normal subgroup of G. Now $N \cap S_i\phi \trianglelefteqslant G$ and $N \cap S_i\phi$ is properly contained in $S_i\phi$ (as $S_i\phi \not\leqslant N$). Therefore, by minimality, $N \cap S_i\phi = \mathbf{1}$. It follows that

$$N \cdot S_i\phi = N \times S_i\phi = S_1 \times S_2 \times \cdots \times S_k \times S_i\phi$$

and

$$N \cdot S_i\phi \trianglelefteqslant G.$$

This shows that $N \cdot S_i\phi \in \mathscr{D}$. This contradicts N being a maximal member of $\mathscr{D}$.

Therefore

$$G = N = S_1 \times S_2 \times \cdots \times S_k,$$

where each S_i is a minimal normal subgroup of G isomorphic to our original minimal normal subgroup S.

It remains to check that S is simple. If $J \trianglelefteqslant S_1$, then

$$J \trianglelefteqslant S_1 \times S_2 \times \cdots \times S_k = G.$$

Therefore, as S_1 is a minimal normal subgroup of G, either $J = \mathbf{1}$ or $J = S_1$. Hence S_1 (and accordingly S) is simple.

Thus the result follows. □

The following key theorem now follows easily:

Theorem 6.28 *A minimal normal subgroup of a finite group G is a direct product of isomorphic simple groups.*

PROOF: By Lemma 6.26, a minimal normal subgroup N of G is characteristically simple. By Theorem 6.27, the group N is therefore a direct product of isomorphic simple groups. □

In a finite soluble group, a minimal normal subgroup is therefore a direct product of cyclic groups of order p (for some prime p).

Definition 6.29 Suppose that p is a prime number. An *elementary abelian p-group* G is an abelian group such that

$$x^p = 1 \qquad \text{for all } x \in G.$$

Recall that a finite abelian group is a direct product of cyclic groups. It follows that a finite group is an elementary abelian p-group if and only if

$$G \cong \underbrace{C_p \times C_p \times \cdots \times C_p}_{d \text{ times}}$$

for some d.

Putting together Theorem 6.18 and Theorem 6.28 gives:

Theorem 6.30 *A minimal normal subgroup of a finite soluble group is an elementary abelian p-group for some prime number p.* □

Example 6.31 (i) The group S_4 has minimal normal subgroup V_4: we have already noted that V_4 is characteristically simple (Example 6.25). It is clear that V_4 is an elementary abelian 2-group.

(ii) Let $G = Q_8$. Then all proper normal subgroups of G contain -1, so $\langle -1 \rangle$ is the unique minimal normal subgroup of G. Since $\langle -1 \rangle \cong C_2$, it is clear that it is an elementary abelian 2-group.

6.2.2 Hall subgroups

Definition 6.32 Let π be a set of prime numbers and let G be a finite group. A *Hall π-subgroup* of G is a subgroup H of G such that $|H|$ is a product involving only the primes in π and $|G : H|$ is a product involving only primes not in π. A subgroup of G is called a *π-subgroup* if its order is a product involving only the primes in π.

If p is a prime number, then a Hall $\{p\}$-subgroup is precisely the same thing as a Sylow p-subgroup.

Example 6.33 Consider the alternating group A_5 of degree 5. Here

$$|A_5| = 60 = 2^2 \cdot 3 \cdot 5.$$

So a Hall $\{2, 3\}$-subgroup of A_5 has order 12. We already know of a subgroup with this order: thus, A_4 is a Hall $\{2, 3\}$-subgroup of A_5.

A Hall $\{2, 5\}$-subgroup of A_5 would have order 20 and index 3, while a Hall $\{3, 5\}$-subgroup of A_5 would have order 15 and index 4. If H were one of these, then we could let A_5 act on the cosets of H and obtain a homomorphism $\rho\colon A_5 \to S_r$ (where $r = 3$ or 4). Here $\ker \rho \neq \mathbf{1}$ and $\ker \rho \neq A_5$ (as $\ker \rho \leqslant H$), which would contradict the fact that A_5 is simple.

Hence A_5 does not have any Hall $\{2, 5\}$-subgroups or Hall $\{3, 5\}$-subgroups.

So in insoluble groups, some Hall π-subgroups might exist, while others might not (in fact, it is a theorem that some definitely do not!). This is in stark contrast to soluble groups:

Theorem 6.34 (P. Hall, 1928) *Let G be a finite soluble group and let π be a set of prime numbers. Then*

(i) *G has a Hall π-subgroup;*

(ii) *any two Hall π-subgroups of G are conjugate;*

(iii) *any π-subgroup of G is contained in a Hall π-subgroup.*

There is a clear analogy between this and Sylow's Theorem (3.4).

Hall subgroups and this theorem are named after Philip Hall (1904–1982), a British mathematician who did groundbreaking research into the theory of finite and infinite groups in the early and mid-parts of the twentieth century.

A number of tools are needed in the course of this theorem. The one remaining fact that has not already been established is the following result.

Lemma 6.35 (Frattini Argument) *Let G be a finite group, N be a normal subgroup of G and P be a Sylow p-subgroup of N. Then*

$$G = \mathrm{N}_G(P)\, N.$$

The name of the lemma suggests (correctly) that it is the method of proof that is actually most important here. The idea can be adapted to many situations and turns out to be very useful.

PROOF: Let $x \in G$. Since $N \trianglelefteq G$,

$$P^x \leqslant N^x = N,$$

so P^x is a Sylow p-subgroup of N. Sylow's Theorem then tells us that P^x and P are conjugate in N:

$$P^x = P^n \qquad \text{for some } n \in N.$$

Therefore

$$P^{xn^{-1}} = P,$$

so $y = xn^{-1} \in \mathrm{N}_G(P)$. Hence $x = yn \in \mathrm{N}_G(P)N$. The reverse inclusion is obvious, so

$$G = \mathrm{N}_G(P)N.$$

□

PROOF OF THEOREM 6.34: Our strategy is to prove part (i) and deduce part (iii) by showing that a π-subgroup is contained in a conjugate of the Hall π-subgroup found already. We will then deduce part (ii) at the end.

We will prove the following by induction on the order of G:

- G has a Hall π-subgroup H;
- if L is a π-subgroup of G then L is contained in some conjugate of H.

Both are trivial if $|G| = 1$. Assume then that $|G| > 1$ and that these statements hold for soluble groups of order smaller than G. Write $|G| = mn$ where m is a product involving primes in π and n is a product involving primes not in π. (A Hall π-subgroup of G is then a subgroup of order m.) We can assume that $m > 1$ since otherwise the statements are trivially true.

Let M be a minimal normal subgroup of G. By Theorem 6.30, M is elementary abelian. We consider two cases according to the prime dividing the order of M.

Case 1: M is an elementary abelian p-group where $p \in \pi$. Write $|M| = p^\alpha$. Then

$$|G/M| = mn/p^\alpha = m_1 n,$$

where $m = m_1 p^\alpha$. By induction, the above statements hold for G/M. The Correspondence Theorem tells us that a Hall π-subgroup of G/M has the form H/M where H is a subgroup of G containing M. Then

$$|H/M| = m_1$$

so

$$|H| = m_1|M| = m_1 p^\alpha = m.$$

Hence H is a Hall π-subgroup of G.

Now let L be any π-subgroup of G. The image LM/M ($\cong L/(L \cap M)$) of L in the quotient group is a π-subgroup of G/M. Hence, by induction, some conjugate of H/M contains LM/M, say

$$LM/M \leqslant (H/M)^{Mx} = H^x/M$$

where $x \in G$. Thus

$$L \leqslant LM \leqslant H^x.$$

This completes Case 1.

Case 2: No minimal normal subgroup of G is an elementary abelian p-group with $p \in \pi$. In particular, our minimal normal subgroup M of G satisfies $|M| = q^\beta$ where $q \notin \pi$. Then

$$|G/M| = mn/q^\beta = mn_1$$

where $n = n_1 q^\beta$. We now further subdivide according to n_1.

Subcase 2A: $n_1 \neq 1$.

By induction, G/M has a Hall π-subgroup, which has the form K/M where K is a subgroup of G containing M and

$$|K/M| = m.$$

Then

$$|K| = m|M| = mq^\beta = mn/n_1 < mn.$$

Now, $|K| < |G|$ and hence by induction K possesses a Hall π-subgroup. Let H be a Hall π-subgroup of K. Then $|H| = m$, so H is also a Hall π-subgroup of G.

Now let L be a π-subgroup of G. The image LM/M of L in the quotient group is a π-subgroup of G/M. Hence, by induction, LM/M is contained in some conjugate of K/M; say

$$LM/M \leqslant (K/M)^{Mx} = K^x/M$$

where $x \in G$. Hence $L \leqslant LM \leqslant K^x$, so $L^{x^{-1}} \leqslant K$. Then $L^{x^{-1}}$ is a π-subgroup of K and since $|K| < |G|$, we deduce by induction that $L^{x^{-1}} \leqslant H^y$ for some $y \in K$. Hence

$$L \leqslant H^{yx}$$

and we have completed Subcase 2A.

Subcase 2B: $n_1 = 1$, so $|G| = mq^\beta$.

Note also that the general assumption of Case 2 still applies: G has no minimal normal subgroup which is an elementary abelian p-group for $p \in \pi$.

Now $|G/M| = m > 1$. Let N/M be a minimal normal subgroup of G/M. Then N/M is an elementary abelian p-group for some $p \in \pi$ (since m is a product involving only primes in π), say $|N/M| = p^\alpha$. Then $N \trianglelefteqslant G$ and

$$|N| = p^\alpha q^\beta.$$

Let P be a Sylow p-subgroup of N. Let us now apply the Frattini Argument (Lemma 6.35):

$$G = \mathrm{N}_G(P)N.$$

But $N = PM$, so

$$G = \mathrm{N}_G(P)PM = \mathrm{N}_G(P)M$$

(as $P \leqslant \mathrm{N}_G(P)$).

Now consider $J = \mathrm{N}_G(P) \cap M$. We will prove that $J = \mathbf{1}$. Since M is abelian, $J \trianglelefteqslant M$. Also since $M \trianglelefteqslant G$, $J = \mathrm{N}_G(P) \cap M \trianglelefteqslant \mathrm{N}_G(P)$. Hence

$$J \trianglelefteqslant \mathrm{N}_G(P)M = G.$$

But M is a minimal normal subgroup of G, so $J = \mathbf{1}$ or $J = M$. If $J = \mathrm{N}_G(P) \cap M = M$, then $M \leqslant \mathrm{N}_G(P)$, so $G = \mathrm{N}_G(P)$. Hence P is a normal p-subgroup of G and some subgroup of P is a minimal normal subgroup of G and this is then an elementary abelian p-group with $p \in \pi$. This is contrary to the general assumption made for Case 2.

Thus $J = \mathbf{1}$, so $\mathrm{N}_G(P) \cap M = \mathbf{1}$. Now

$$mq^\beta = |G| = |\mathrm{N}_G(P)M| = |\mathrm{N}_G(P)| \cdot |M|,$$

so $|\mathrm{N}_G(P)| = m$. Hence $H = \mathrm{N}_G(P)$ is our Hall π-subgroup. (We have now completed part (i) of the theorem!)

Now consider some π-subgroup L of G. We have shown already that $G = HM$, so

$$\begin{aligned} LM &= LM \cap G \\ &= LM \cap HM \\ &= (LM \cap H)M \end{aligned}$$

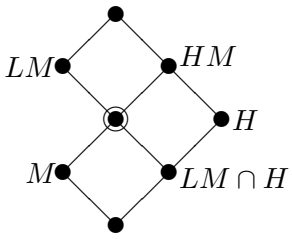

Figure 6.1: Subcase 2B: $LM \cap HM = (LM \cap H)M$

by Dedekind's Modular Law (Lemma 1.9). Now $LM \cap H$ is a π-group (as a subgroup of H) and

$$\begin{aligned} |LM : LM \cap H| &= \frac{|(LM \cap H)M|}{|LM \cap H|} \\ &= \frac{|M|}{|LM \cap H \cap M|} = |M| \end{aligned}$$

(since $H \cap M = \mathbf{1}$ as they have coprime order). Hence $LM \cap H$ is a Hall π-subgroup of LM.

If $LM < G$, we can apply induction to the group LM to see that some conjugate of the Hall π-subgroup $LM \cap H$ contains the π-subgroup L:

$$L \leqslant (LM \cap H)^x \leqslant H^x$$

for some $x \in G$ (indeed we could pick $x \in LM$). We would then be done.

So suppose $LM = G$. Then as $L \cap M = \mathbf{1}$ (they have coprime order),

$$|G| = |LM| = |L| \cdot |M|,$$

so $|L| = mq^\beta/q^\beta = m$. Also, $M \leqslant N$, so $G = LM = LN$. Thus

$$|G| = |LN| = \frac{|L| \cdot |N|}{|L \cap N|},$$

so

$$|L \cap N| = \frac{|L| \cdot |N|}{|G|} = \frac{m \cdot p^\alpha q^\beta}{mq^\beta} = p^\alpha.$$

Thus $L \cap N$ is a Sylow p-subgroup of N. By Sylow's Theorem, it is conjugate to the Sylow p-subgroup P which we already know about, say

$$L \cap N = P^x \qquad \text{where } x \in N \leq G.$$

Now $L \cap N \trianglelefteqslant L$, since $N \trianglelefteq G$, so

$$L \leqslant \mathrm{N}_G(L \cap N) = \mathrm{N}_G(P^x) = \mathrm{N}_G(P)^x = H^x.$$

Thus L is contained in some conjugate of our Hall π-subgroup H. This completes the proof of (i) and (iii).

We have now shown that if G is a finite soluble group, then G has a Hall π-subgroup H, and every π-subgroup of G is contained in a conjugate of H. It remains to prove (ii). Let K be any Hall π-subgroup of G. By (iii), $K \leqslant H^x$ for some $x \in G$. But these subgroups have the same order, so we deduce $K = H^x$ and so part (ii) of Theorem 6.34 holds.

This completes the proof of Hall's Theorem. □

6.2.3 Sylow systems and Sylow bases

We now examine some consequences of Hall's Theorem. Specifically, we will see how the Sylow subgroups of a soluble group can be arranged to have special properties.

Definition 6.36 If $p \in \mathbb{N}$ is prime, write p' for the set of all primes not equal to p. A Hall p'-subgroup of a finite group G is a *p-complement*.

Note that $2'$ then denotes the set of all odd primes.

Let G be a finite group, with $|G| = p^n m$ where p does not divide m. Then a Hall p'-subgroup H has order m, while a Sylow p-subgroup P has order p^n. As they have coprime orders, we see $H \cap P = \mathbf{1}$ and therefore

$$|HP| = |H| \cdot |P| = |G|,$$

so

$$G = HP, \quad H \cap P = \mathbf{1}.$$

In this situation H and P are complements to one another (see Definition 5.9), although neither subgroup is necessarily normal.

Example 6.37 Consider $D_{2\times 15}$. A Hall $2'$-subgroup has order $30/2 = 15$, so the subgroup $\langle\alpha\rangle$ is a complement to the Sylow 2-subgroup $\langle\beta\rangle$ of $D_{2\times 15}$.

Let G be a finite soluble group and write

$$|G| = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$$

where $p_1, p_2, \dots, p_k$ are the distinct prime factors of $|G|$. By Hall's Theorem, G has a Hall p'-subgroup for each prime. Let Q_1, Q_2, …, Q_k be Hall p_i'-subgroups for $i = 1, 2, \dots, k$, respectively. Then

$$|Q_i| = |G|/p_i^{n_i} \qquad \text{and} \qquad |G : Q_i| = p_i^{n_i}.$$

Claim: $Q_1 \cap Q_2 \cap \cdots \cap Q_t$ is a Hall $\{p_{t+1}, \ldots, p_k\}$-subgroup of G.

PROOF OF CLAIM: This is certainly true when $t = 1$. Assume inductively that the intersection $H = Q_1 \cap Q_2 \cap \cdots \cap Q_t$ is a Hall $\{p_{t+1}, \ldots, p_k\}$-subgroup of G. Then

$$|H| = p_{t+1}^{n_{t+1}} \ldots p_k^{n_k} \qquad \text{and} \qquad |G : H| = p_1^{n_1} \ldots p_t^{n_t}.$$

Now apply Lemma 1.14: H and Q_{t+1} have coprime indices, so

$$|G : H \cap Q_{t+1}| = |G : H| \cdot |G : Q_{t+1}| = p_1^{n_1} \ldots p_t^{n_t} p_{t+1}^{n_{t+1}}.$$

Hence $|H \cap Q_{t+1}| = p_{t+2}^{n_{t+2}} \ldots p_k^{n_k}$, so $H \cap Q_{t+1} = Q_1 \cap \cdots \cap Q_{t+1}$ is a Hall $\{p_{t+2}, \ldots, p_k\}$-subgroup of G. Thus the claim holds by induction. □

In particular, $P_k = Q_1 \cap Q_2 \cap \cdots \cap Q_{k-1}$ is a Hall $\{p_k\}$-subgroup of G; that is, a Sylow p_k-subgroup of G. Generalising in the obvious way, we deduce that

$$P_r = \bigcap_{i \neq r} Q_i$$

is a Sylow p_r-subgroup of G (for $r = 1, 2, \ldots, k$).

Now consider the two Sylow subgroups P_{k-1} and P_k. Firstly $P_{k-1} \cap P_k = \mathbf{1}$ (since they have coprime orders), so

$$|P_{k-1}P_k| = |P_{k-1}| \cdot |P_k| = p_{k-1}^{n_{k-1}} p_k^{n_k} = |P_k P_{k-1}|.$$

Further, by construction, both P_{k-1} and P_k are contained in the intersection $Q_1 \cap Q_2 \cap \cdots \cap Q_{k-2}$ and by our claim this intersection is a Hall $\{p_{k-1}, p_k\}$-subgroup of G; that is,

$$|Q_1 \cap Q_2 \cap \cdots \cap Q_{k-2}| = p_{k-1}^{n_{k-1}} p_k^{n_k}.$$

Since it is a subgroup, this Hall subgroup is closed under products, so

$$P_{k-1}P_k,\ P_k P_{k-1} \subseteq Q_1 \cap Q_2 \cap \cdots \cap Q_{k-2}.$$

Finally the subsets occurring in the previous inclusion all have the same size, so we deduce

$$P_{k-1}P_k = Q_1 \cap Q_2 \cap \cdots \cap Q_{k-2} = P_k P_{k-1}.$$

Generalising in the obvious way, we deduce that for all $r \neq s$:

$$P_r P_s = P_s P_r.$$

Definition 6.38 Let G be a finite group and let $p_1, p_2, \ldots, p_k$ be the distinct prime factors of $|G|$.

(i) A *Sylow system* for G is a collection $Q_1, Q_2, \ldots, Q_k$ such that Q_i is a Hall p_i'-subgroup of G (for $i = 1, 2, \ldots, k$).

(ii) A *Sylow basis* for G is a collection $P_1, P_2, \ldots, P_k$ such that P_i is a Sylow p_i-subgroup of G (for $i = 1, 2, \ldots, k$) and such that

$$P_i P_j = P_j P_i \qquad \text{for all } i \text{ and } j.$$

We have shown:

Theorem 6.39 *A finite soluble group possesses a Sylow system and a Sylow basis.* □

Recall that the product HK of two subgroups is a subgroup if and only if $HK = KH$. Consequently, if we start with a Sylow basis $P_1, P_2, \ldots, P_k$ for a finite soluble group G, then we can form

$$P_{i_1} P_{i_2} \ldots P_{i_s}$$

for any subset $\{i_1, i_2, \ldots, i_s\} \subseteq \{1, 2, \ldots, k\}$. The fact that the Sylow subgroups in our Sylow basis permute ensures that this is a subgroup and it is easy to see that its order is $p_{i_1}^{n_{i_1}} p_{i_2}^{n_{i_2}} \ldots p_{i_s}^{n_{i_s}}$. Thus we have formed a Hall subgroup for the appropriate collection of primes. Hence a Sylow basis is a nice collection of Sylow subgroups from which we may easily construct Hall subgroups.

Philip Hall proved far more than these results. The final two theorems of this section will not be proved: the first appears on Tutorial Sheet VI.

Theorem 6.40 (P. Hall) *Let G be a finite soluble group. Then any two Sylow bases for G are conjugate (that is, if $P_1, P_2, \ldots, P_k$ and $R_1, R_2, \ldots, R_k$ are two Sylow bases for G, where P_i and R_i are Sylow subgroups for the same prime, then there exists $x \in G$ such that $R_i = P_i^x$ for all i).*

This is much stronger than Sylow's Theorem. The latter tells us that each R_i is a conjugate of P_i. What the above theorem tells us is that when the Sylow subgroups come from a Sylow basis then we can actually choose the same element x to conjugate all the Sylow subgroups simultaneously.

Finally we have the following major converse to Hall's Theorem.

Theorem 6.41 (P. Hall) *Let G be a finite group which possesses a Hall p'-subgroup for every prime p. Then G is soluble.*

Putting Theorems 6.34 and 6.41 together, we see that a group is soluble if and only if it has Hall π-subgroups for all collections π of primes. (In particular, our observation that A_5 was missing some Hall subgroups is no longer surprising.)