Definition. A group G is *solvable* if there is a chain of subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_s = G$$

such that G_{i+1}/G_i is abelian for $i = 0, 1, \ldots, s-1$.

The terminology comes from the correspondence in Galois Theory between these groups and polynomials which can be solved by radicals (which essentially means there is an algebraic formula for the roots). Exercise 8 shows that finite solvable groups are precisely those groups whose composition factors are all of prime order.

One remarkable property of finite solvable groups is the following generalization of Sylow's Theorem due to Philip Hall (cf. Theorem 6.11 and Theorem 19.8).

Theorem. The finite group G is solvable if and only if for every divisor n of $|G|$ such that $(n, \frac{|G|}{n}) = 1$, G has a subgroup of order n.

As another illustration of how properties of a group G can be deduced from combined information from a normal subgroup N and the quotient group G/N we prove

if N and G/N are solvable, then G is solvable.

To see this let $\overline{G} = G/N$, let $1 = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_n = N$ be a chain of subgroups of N such that N_{i+1}/N_i is abelian, $0 \le i < n$ and let $\overline{1} = \overline{G_0} \trianglelefteq \overline{G_1} \trianglelefteq \ldots \trianglelefteq \overline{G_m} = \overline{G}$ be a chain of subgroups of $\overline{G}$ such that $\overline{G_{i+1}}/\overline{G_i}$ is abelian, $0 \le i < m$. By the Lattice Isomorphism Theorem there are subgroups G_i of G with $N \le G_i$ such that $G_i/N = \overline{G_i}$ and $G_i \trianglelefteq G_{i+1}$, $0 \le i < m$. By the Third Isomorphism Theorem

$$\overline{G_{i+1}}/\overline{G_i} = (G_{i+1}/N)/(G_i/N) \cong G_{i+1}/G_i.$$

Thus

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_n = N = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_m = G$$

is a chain of subgroups of G all of whose successive quotient groups are abelian. This proves G is solvable.

It is inaccurate to say that finite group theory is concerned *only* with the Hölder Program. It *is* accurate to say that the Hölder Program suggests a large number of problems and motivates a number of algebraic techniques. For example, in the study of the extension problem where we are given groups A and B and wish to find G and $N \trianglelefteq G$ with $N \cong B$ and $G/N \cong A$, we shall see that (under certain conditions) we are led to an *action* of the group A on the set B. Such actions form the crux of the next chapter (and will result in information both about simple and non-simple groups) and this notion is a powerful one in mathematics not restricted to the theory of groups.

The final section of this chapter introduces another family of groups and although in line with our interest in simple groups, it will be of independent importance throughout the text, particularly in our study later of determinants and the solvability of polynomial equations.

is called the *lower central series of* G. (The term "lower" indicates that $G^i \geq G^{i+1}$.)

As with the upper central series we include in the exercises at the end of this section the verification that G^i is a characteristic subgroup of G for all i. The next theorem shows the relation between the upper and lower central series of a group.

Theorem 8. A group G is nilpotent if and only if $G^n = 1$ for some $n \geq 0$. More precisely, G is nilpotent of class c if and only if c is the smallest nonnegative integer such that $G^c = 1$. If G is nilpotent of class c then

$$Z_i(G) \leq G^{c-i-1} \leq Z_{i+1}(G) \quad \text{for all } i \in \{0, 1, \ldots, c-1\}.$$

Proof: This is proved by a straightforward induction on the length of either the upper or lower central series.

The terms of the upper and lower central series do not necessarily coincide in general although in some groups this does occur.

Remarks:

(1) If G is abelian, we have already seen that $G' = G^1 = 1$ so the lower central series terminates in the identity after one term.

(2) As with the upper central series, for any finite group there must, by order considerations, be an integer n such that

$$G^n = G^{n+1} = G^{n+2} = \cdots.$$

For non-nilpotent groups, G^n is a nontrivial subgroup of G. For example, in Section 5.4 we showed that $S_3' = S_3^1 = A_3$. Since S_3 is not nilpotent, we must have $S_3^2 = A_3$. In fact

$$(123) = [(12), (132)] \in [S_3, S_3^1] = S_3^2.$$

Once two terms in the lower central series are the same, the chain stabilizes at that point i.e., all terms thereafter are equal to these two. Thus $S_3^i = A_3$ for all $i \geq 2$. Note that S_3 is an example where the lower central series has two distinct terms whereas all terms in the upper central series are equal to the identity (in particular, for non-nilpotent groups these series need not have the same length).

Solvable Groups and the Derived Series

Recall that in Section 3.4 a solvable group was defined as one possessing a series:

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_s = G$$

such that each factor H_{i+1}/H_i is abelian. We now give another characterization of solvability in terms of a descending series of characteristic subgroups.

Definition. For any group G define the following sequence of subgroups inductively:

$$G^{(0)} = G, \qquad G^{(1)} = [G, G] \quad \text{and} \quad G^{(i+1)} = [G^{(i)}, G^{(i)}] \quad \text{for all } i \geq 1.$$

This series of subgroups is called the *derived* or *commutator* series of G.

The terms of this series are also often written as: $G^{(1)} = G'$, $G^{(2)} = G''$, etc. Again it is left as an exercise to show that each $G^{(i)}$ is characteristic in G for all i.

It is important to note that although $G^{(0)} = G^0$ and $G^{(1)} = G^1$, it is not in general true that $G^{(i)} = G^i$. The difference is that the definition of the $i+1^{\text{st}}$ term in the lower central series is the commutator of the i^{th} term with the *whole* group G whereas the $i+1^{\text{st}}$ term in the derived series is the commutator of the i^{th} term with itself. Hence

$$G^{(i)} \leq G^i \quad \text{for all } i$$

and the containment can be proper. For example, in $G = S_3$ we have already seen that $G^1 = G' = A_3$ and $G^2 = [S_3, A_3] = A_3$, whereas $G^{(2)} = [A_3, A_3] = 1$ (A_3 being abelian).

Theorem 9. A group G is solvable if and only if $G^{(n)} = 1$ for some $n \geq 0$.

Proof: Assume first that G is solvable and so possesses a series

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_s = G$$

such that each factor H_{i+1}/H_i is abelian. We prove by induction that $G^{(i)} \leq H_{s-i}$. This is true for $i = 0$, so assume $G^{(i)} \leq H_{s-i}$. Then

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] \leq [H_{s-i}, H_{s-i}].$$

Since H_{s-i}/H_{s-i-1} is abelian, by Proposition 5.7(4), $[H_{s-i}, H_{s-i}] \leq H_{s-i-1}$. Thus $G^{(i+1)} \leq H_{s-i-1}$, which completes the induction. Since $H_0 = 1$ we have $G^{(s)} = 1$.

Conversely, if $G^{(n)} = 1$ for some $n \geq 0$, Proposition 5.7(4) shows that if we take H_i to be $G^{(n-i)}$ then H_i is a normal subgroup of H_{i+1} with abelian quotient, so the derived series itself satisfies the defining condition for solvability of G. This completes the proof.

If G is solvable, the smallest nonnegative n for which $G^{(n)} = 1$ is called the *solvable length* of G. The derived series is a series of shortest length whose successive quotients are abelian and it has the additional property that it consists of subgroups that are characteristic in the *whole* group (as opposed to each just being normal in the *next* in the initial definition of solvability). Its "intrinsic" definition also makes it easier to work with in many instances, as the following proposition (which reproves some results and exercises from Section 3.4) illustrates.

Proposition 10. Let G and K be groups, let H be a subgroup of G and let $\varphi : G \to K$ be a surjective homomorphism.

(1) $H^{(i)} \leq G^{(i)}$ for all $i \geq 0$. In particular, if G is solvable, then so is H, i.e., subgroups of solvable groups are solvable (and the solvable length of H is less than or equal to the solvable length of G).

(2) $\varphi(G^{(i)}) = K^{(i)}$. In particular, homomorphic images and quotient groups of solvable groups are solvable (of solvable length less than or equal to that of the domain group).
(3) If N is normal in G and both N and G/N are solvable then so is G.

Proof: Part 1 follows from the observation that since $H \leq G$, by definition of commutator subgroups, $[H, H] \leq [G, G]$, i.e., $H^{(1)} \leq G^{(1)}$. Then, by induction,

$$H^{(i)} \leq G^{(i)} \quad \text{for all } i \in \mathbb{Z}^+.$$

In particular, if $G^{(n)} = 1$ for some n, then also $H^{(n)} = 1$. This establishes (1).

To prove (2) note that by definition of commutators,

$$\varphi([x, y]) = [\varphi(x), \varphi(y)]$$

so by induction $\varphi(G^{(i)}) \leq K^{(i)}$. Since φ is surjective, every commutator in K is the image of a commutator in G, hence again by induction we obtain equality for all i. Again, if $G^{(n)} = 1$ for some n then $K^{(n)} = 1$. This proves (2).

Finally, if G/N and N are solvable, of lengths n and m respectively then by (2) applied to the natural projection $\varphi : G \to G/N$ we obtain

$$\varphi(G^{(n)}) = (G/N)^{(n)} = 1N$$

i.e., $G^{(n)} \leq N$. Thus $G^{(n+m)} = (G^{(n)})^{(m)} \leq N^{(m)} = 1$. Theorem 9 shows that G is solvable, which completes the proof.

Some additional conditions under which finite groups are solvable are the following:

Theorem 11. Let G be a finite group.
(1) (Burnside) If $|G| = p^a q^b$ for some primes p and q, then G is solvable.
(2) (Philip Hall) If for every prime p dividing $|G|$ we factor the order of G as $|G| = p^a m$ where $(p, m) = 1$, and G has a subgroup of order m, then G is solvable (i.e., if for all primes p, G has a subgroup whose index equals the order of a Sylow p-subgroup, then G is solvable — such subgroups are called Sylow p-complements).
(3) (Feit–Thompson) If $|G|$ is odd then G is solvable.
(4) (Thompson) If for every pair of elements $x, y \in G$, $\langle x, y \rangle$ is a solvable group, then G is solvable.

We shall prove Burnside's Theorem in Chapter 19 and deduce Philip Hall's generalization of it. As mentioned in Section 3.5, the proof of the Feit–Thompson Theorem takes 255 pages. Thompson's Theorem was first proved as a consequence of a 475 page paper (that in turn relies ultimately on the Feit–Thompson Theorem).

A Proof of the Fundamental Theorem of Finite Abelian Groups

We sketch a group-theoretic proof of the result that every finite abelian group is a direct product of cyclic groups (i.e., Parts 1 and 2 of Theorem 5, Section 5.2) — the Classification of Finitely Generated Abelian Groups (Theorem 3, Section 5.2) will be derived as a consequence of a more general theorem in Chapter 12.