Note first that each P_i is normal in G so $P_1 \cdots P_t$ is a subgroup of G. Let H be the product $P_1 \cdots P_{t-1}$ and let $K = P_t$, so by induction $H \cong P_1 \times \cdots \times P_{t-1}$. In particular, $|H| = |P_1| \cdot |P_2| \cdots |P_{t-1}|$. Since $|K| = |P_t|$, the orders of H and K are relatively prime. Lagrange's Theorem implies $H \cap K = 1$. By definition, $P_1 \cdots P_t = HK$, hence Theorem 5.9 gives

$$HK \cong H \times K = (P_1 \times \cdots \times P_{t-1}) \times P_t \cong P_1 \times \cdots \times P_t$$

which completes the induction. Now take $t = s$ to obtain (4).

Finally, to prove (4) implies (1) use Exercise 1 of Section 5.1 to obtain

$$Z(P_1 \times \cdots \times P_s) \cong Z(P_1) \times \cdots \times Z(P_s).$$

By Exercise 14 in Section 5.1,

$$G/Z(G) = (P_1/Z(P_1)) \times \cdots \times (P_s/Z(P_s)).$$

Thus the hypotheses of (4) also hold for $G/Z(G)$. By Theorem 1, if $P_i \neq 1$ then $Z(P_i) \neq 1$, so if $G \neq 1$, $|G/Z(G)| < |G|$. By induction, $G/Z(G)$ is nilpotent, so by Exercise 6, G is nilpotent. This completes the proof.

Note that the first part of the Fundamental Theorem of Finite Abelian Groups (Theorem 5 in Section 5.2) follows immediately from the above theorem (we shall give another proof later as a consequence of the Chinese Remainder Theorem):

Corollary 4. A finite abelian group is the direct product of its Sylow subgroups.

Next we prove a proposition which will be used later to show that the multiplicative group of a finite field is cyclic (without using the Fundamental Theorem of Finite Abelian Groups).

Proposition 5. If G is a finite group such that for all positive integers n dividing its order, G contains at most n elements x satisfying $x^n = 1$, then G is cyclic.

Proof: Let $|G| = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ and let P_i be a Sylow p_i-subgroup of G for $i = 1, 2, \dots, s$. Since $p_i^{\alpha_i} \mid |G|$ and the $p_i^{\alpha_i}$ elements of P_i are solutions of $x^{p_i^{\alpha_i}} = 1$, by hypothesis P_i must contain *all* solutions to this equation in G. It follows that P_i is the unique (hence normal) Sylow p_i-subgroup of G. By Theorem 3, G is the direct product of its Sylow subgroups. By Theorem 1, each P_i possesses a normal subgroup M_i of index p_i. Since $|M_i| = p_i^{\alpha_i - 1}$ and G has at most $p_i^{\alpha_i - 1}$ solutions to $x^{p_i^{\alpha_i - 1}} = 1$, by Lagrange's Theorem (Corollary 9, Section 3.2) M contains all elements x of G satisfying $x^{p_i^{\alpha_i - 1}} = 1$. Thus any element of P_i not contained in M_i satisfies $x^{p_i^{\alpha_i}} = 1$ but $x^{p_i^{\alpha_i - 1}} \neq 1$, i.e., x is an element of order $p_i^{\alpha_i}$. This proves P_i is cyclic for all i, so G is the direct product of cyclic groups of relatively prime order, hence is cyclic.

The next proposition is called Frattini's Argument. We shall apply it to give another characterization of finite nilpotent groups. It will also be a valuable tool in the next section.

Proposition 6. *(Frattini's Argument)* Let G be a finite group, let H be a normal subgroup of G and let P be a Sylow p-subgroup of H. Then $G = HN_G(P)$ and $|G : H|$ divides $|N_G(P)|$.

Proof: By Corollary 3.15, $HN_G(P)$ is a subgroup of G and $HN_G(P) = N_G(P)H$ since H is a normal subgroup of G. Let $g \in G$. Since $P^g \leq H^g = H$, both P and P^g are Sylow p-subgroups of H. By Sylow's Theorem applied in H, there exists $x \in H$ such that $P^g = P^x$. Thus $gx^{-1} \in N_G(P)$ and so $g \in N_G(P)x$. Since g was an arbitrary element of G, this proves $G = N_G(P)H$.

Apply the Second Isomorphism Theorem to $G = N_G(P)H$ to conclude that

$$|G : H| = |N_G(P) : N_G(P) \cap H|$$

so $|G : H|$ divides $|N_G(P)|$, completing the proof.

Proposition 7. A finite group is nilpotent if and only if every maximal subgroup is normal.

Proof: Let G be a finite nilpotent group and let M be a maximal subgroup of G. As in the proof of Theorem 1, since $M < N_G(M)$ (by Theorem 3(2)) maximality of M forces $N_G(M) = G$, i.e., $M \trianglelefteq G$.

Conversely, assume every maximal subgroup of the finite group G is normal. Let P be a Sylow p-subgroup of G. We prove $P \trianglelefteq G$ and conclude that G is nilpotent by Theorem 3(3). If P is not normal in G let M be a maximal subgroup of G containing $N_G(P)$. By hypothesis, $M \trianglelefteq G$ hence by Frattini's Argument $G = MN_G(P)$. Since $N_G(P) \leq M$ we have $MN_G(P) = M$, a contradiction. This establishes the converse.

Commutators and the Lower Central Series

For the sake of completeness we include the definition of the *lower central series* of a group and state its relation to the upper central series. Since we shall not be using these results in the future, the proofs are left as (straightforward) exercises.

Recall that the commutator of two elements x, y in a group G is defined as

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

and the commutator of two subgroups H and K of G is

$$[H, K] = \langle [h, k] \mid h \in H, \ k \in K \rangle.$$

Basic properties of commutators and the commutator subgroup were established in Section 5.4.

Definition. For any (finite or infinite) group G define the following subgroups inductively:

$$G^0 = G, \qquad G^1 = [G, G] \quad \text{and} \quad G^{i+1} = [G, G^i].$$

The chain of groups

$$G^0 \geq G^1 \geq G^2 \geq \cdots$$

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

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

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 $\varphi : G \twoheadrightarrow K$ 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).