Subnormal series continued

After so many definitions, we need examples.

Example: Every group G always has at least one subnormal series: $G_0 = G$ and $G_1 = \{id\}$.

If G is simple, this is the only series.

Example: The group D_4 has several subnormal series, for example if $D_4 = \langle r, s \mid r^4 = 1, s^2 = 1 \text{ and } srs = r^{-1} \rangle$

then $srs = r^{-1} \Rightarrow s^2rs = sr^{-1}$

$$\Rightarrow s^2 rs(s^{-1}) = sr^{-1}s^{-1} \Rightarrow sr^{-1}s^{-1} = r, \text{ and } sr^2s^{-1} = r^{2}$$

so the subgroup $\langle r^2 \rangle$ is normal in D_4. Thus

(i) $D_4 \geq \langle r^2 \rangle \geq \{id\}$

is one subnormal series. There are also series:

(ii) $D_4 \geq \langle r \rangle \geq \langle r^2 \rangle \geq \{id\}$

(iii) $D_4 \geq \langle r^2, s \rangle \geq \langle s \rangle \geq \{id\}$

The factors of series (i) are $D_4/\langle r^2 \rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ and $\langle r^2 \rangle / \{id\} \simeq \langle r^2 \rangle \simeq \mathbb{Z}_2$.

Series (ii) is a one-step refinement of (i).

Its factors are $D_4/\langle r \rangle \simeq \mathbb{Z}_2$, $\langle r \rangle / \langle r^2 \rangle \simeq \mathbb{Z}_2$,

$$\langle r^2 \rangle / \{id\} \simeq \langle r^2 \rangle \simeq \mathbb{Z}_2.$$

Series (iii) has the same factors as (ii).

Note that (ii) and (iii) are also composition series since each factor is simple, and solvable series since each factor is abelian.

<u>Remark</u>: Note that the series

$$D_4 \trianglerighteq \langle r \rangle \trianglerighteq \langle r^2 \rangle \trianglerighteq \{id\}$$

has no refinement. If it did, say

$$D_4 \trianglerighteq \langle r \rangle \trianglerighteq N \trianglerighteq \langle r^2 \rangle \trianglerighteq \{id\}.$$

then under the quotient $\varphi : \langle r \rangle \longrightarrow \langle r \rangle / \langle r^2 \rangle$

the image $\varphi(N)$ would be a normal subgroup, but this is not possible since $\langle r \rangle / \langle r^2 \rangle \simeq \mathbb{Z}_2$.

This is true of composition series in general:

Suppose $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n$ is a composition series. If $G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_i \trianglerighteq N \trianglerighteq G_{i+1} \trianglerighteq \cdots \trianglerighteq G_n$ is a refinement, then $\varphi : G_i \longrightarrow G_i / G_{i+1}$ yields a normal subgroup $\varphi(N) \subseteq G_i / G_{i+1}$. Then $\varphi(N) = \{id\}$ or $\varphi(N) = G_i / G_{i+1}$ since G_i / G_{i+1} is simple, so a composition series has no proper refinements.

<u>Example</u>: Suppose $G \simeq \mathbb{Z}$. Then G has no composition series.

To see this, not every subgroup $G_i \subset \mathbb{Z}$ is isomorphic to $\mathbb{Z}$. Thus if we have

$$\mathbb{Z} = G_0 \geq G_1 \geq \cdots$$

then $G_i \cong \mathbb{Z}$ for all i so we cannot have $G_n = \{id\}$ for some n.

<u>Theorem</u>: Every finite group has a composition series.

<u>Proof</u>: Let G be finite. Then $G = G_0 \geq G_1 = \{id\}$ is a subnormal series. If G is not simple then it's <u>not</u> a composition series, so $\exists\, N \triangleleft G$. Then the refinement $G = G_0 \geq N \geq G = \{id\}$ is a proper refinement, and if this is not a composition series then it admits yet another proper refinement...

If general, if G_i/G_{i+1} is <u>not</u> simple then there's $N \subset G$ with $G_{i+1} \triangleleft N \triangleleft G_i$ yielding a proper refinement of our previous series.

Since the length of a series of G is bounded above by $|G|$, this process must terminate. A series which has no further refinements is then a composition series, completing the proof.

<u>Theorem</u>: Every refinement of a solvable series is solvable. A group is solvable if and only if it has a solvable series.

<u>Proof</u>. First suppose $G = G_0 \geq G_1 \geq \cdots \geq G_n$ is a solvable series and $G_i \geq H > G_{i+1}$ is part of some refinement. We must show H/G_{i+1} and G_i/H are both abelian.

Observe that $H/G_{i+1} \subseteq G_i/G_{i+1}$, so it's abelian. On the other hand the Third isomorphism theorem gives $G_i/H \simeq \left(G_i/G_{i+1}\right)/\left(H/G_{i+1}\right)$, so G_i/H is a quotient of the abelian group G_i/G_{i+1}, hence abelian. So refinements of solvable series are solvable.

Next suppose G is solvable. Then $G \geq G^{(1)} \geq G^{(2)} \geq \cdots \geq G^{(n)} = \{id\}$ is a solvable series. On the other hand if $G = G_0 \geq G_1 \geq \cdots \geq G_n = \langle id \rangle$ is a solvable series, then since G/G_1 is abelian we know $G' \subset G_1$. Then G_1/G_2 abeliam implies $G_1' \subset G_2$, combining with $G' \subset G_1 \Rightarrow (G')' \subset G_1'$ this gives $G^{(2)} \subset G_2$. By induction $G^{(n)} \subset G_n = \{id\}$ so G is solvable.

For finite groups, the existence of a solvable series implies something quite strong. As in the proof of "finite groups have composition series", we can take the solvable series of a finite group and refine it until we cannot refine it any more. This means we'll reach a solvable series with simple quotients – ie, cyclic abelian groups of prime order.

<u>Theorem</u>: A finite group G is solvable iff G has a composition series with factors that are cyclic of prime order.

<u>Proof</u>: First, a composition series with factor groups cyclic of prime order is a solvable series. Second suppose
$G = G_0 \geq G_1 \geq \cdots \geq G_n = \{id\}$ is a solvable series for a finite group G. Suppose $G_0 \neq G_1$, then there is a <u>maximal normal subgroup</u> H_1 with $G_1 \leq H_1$, ie a subgroup H_1 with $H_1 \trianglelefteq G$, $G_1 \trianglelefteq H$ and G_0/H_1 simple. Then if H/G_1 is not simple, we choose a maximal normal subgroup H_2, etc. Doing so gives a refinement of the original series:

$$G = G_0 \geq H_1 \geq \cdots \geq H_k \geq G_1 \geq \cdots \geq G_n$$

where each quotient

$$G_0/H, \quad H_i/H_{i+1} \quad \text{and} \quad H_k/G_1 \quad \text{is simple}$$

and each quotient is also abelian:

Every group G_0/H, H_i/H_{i+1} and H_k/G_1 is the image of a subgroup of the abelian group G_0/G_1 under an appropriate quotient homomorphism (e.g. the subgroup H_i/G_1, which is abelian, maps onto H_i/H_{i+1}). Refining the entire series in this way we arrive at $G = N_0 \geq N_1 \geq \cdots \geq N_r = \{id\}$ where each factor is abelian and simple. (Exercise: This means the group is cyclic of prime order).

Exercise hint: In an abelian group, every subgroup is normal. So if it's going to be simple, an abelian group must have no proper, nontrivial subgroups. In particular, if $a \in A$ and $a \neq id$ then $\langle a \rangle = A$ (for all $a \in A$).

Our last definition before tackling the Jordan-Hölder theorem:

Definition: Two subnormal series S and T of a group G are equivalent if there's a bijection between the nontrivial factors of S and the factors of T such that corresponding factors are isomorphic groups.

E.g: We previously saw the two composition series:

$$D_4 \geq \langle r \rangle \geq \langle r^2 \rangle \geq \{id\}$$

and $D_4 \geq \langle r^2, s \rangle \geq \langle s \rangle \geq \{id\}$

and saw that for each, the factors are $\mathbb{Z}_2$, $\mathbb{Z}_2$ and $\mathbb{Z}_2$.
So these series are equivalent.

<u>Observation</u>: If S is a composition series, then any refinement of S is equivalent to S — because, as we already saw, S has no proper refinements. So any <u>refinement</u> of S simply has additional trivial factors.

We prepare a first ingredient for the proof of Jordan-Holder:

<u>Lemma</u> (Zassenhaus Lemma)

Let G be a group, and A, A', B, B' subgroups of G.
Suppose $A' \triangleleft A$ and $B' \triangleleft B$. Then:

(i) $A'(A \cap B')$ is normal in $A'(A \cap B)$

(ii) $B'(A' \cap B)$ is normal in $B'(A \cap B)$

(iii) $$\frac{A'(A \cap B)}{A'(A \cap B')} \simeq \frac{B'(A \cap B)}{B'(A' \cap B)}$$

<u>Proofs</u>:

<u>Proof of (i)</u>. Since B' is normal in B,

$A \cap B'$ is normal in $A \cap B$. Note that this means $(A \cap B') = (A \cap B) \cap B'$ is normal in $A \cap B$. By essentially the same argument, $A' \cap B$ is normal in $A \cap B$. So, since both $A \cap B'$ and $A' \cap B$ are normal in $A \cap B$, so is $(A \cap B')(A' \cap B)$. We also have that $A \cap B \leq A$ and $A' \trianglelefteq A$, so $A'(A \cap B)$ is a subgroup of A and $B'(A \cap B)$ is a subgroup of B. Goal to finish: Define an <u>onto</u> homomorphism

$$f: A'(A \cap B) \longrightarrow (A \cap B) / (A \cap B')(A' \cap B)$$

whose kernel is $A'(A \cap B')$. Then the group $A'(A \cap B')$ will be normal in $A'(A \cap B)$, proving (i), and also

$$A'(A \cap B) / A'(A \cap B') \simeq A \cap B / (A \cap B')(A' \cap B)$$

by the first isomorphism theorem. Then, if we succeed in defining such an f we can identically define an onto homomorphism

$$h: B'(A \cap B) \longrightarrow (A \cap B) / (A \cap B')(A' \cap B)$$

with kernel $B'(A' \cap B)$. This proves (ii), and also shows that

$$\frac{B'(A \cap B)}{B'(A' \cap B)} \simeq \frac{(A \cap B)}{(A \cap B')(A' \cap B)},$$

the same thing as above.

Thus (iii) is proved as well, <u>if</u> we construct f as claimed.

Recipe for $f: A'(A\cap B) \longrightarrow (A\cap B)\big/ (A\cap B)(A'\cap B) =: D$, for short.

Given $a \in A'$, $c \in A\cap B$, then ac is an element of the domain. Define $f(ac) = Dc$.

First note f is well-defined, because if $ac = a'c'$ then $c(c')^{-1} = (a')^{-1}a \in (A\cap B)\cap A' = A'\cap B \leq D$, so since $c(c')^{-1} \in D$ we know $Dc = Dc'$. The map is obviously surjective. Finally suppose $ac \in \ker f$, this happens iff $c \in D$, that is, if and only if $c = a'c'$ with $a' \in A'\cap B$ and $c' \in A\cap B'$. Hence $ac \in \ker f$ if and only if $ac = \underset{\underset{A'}{\cap}}{(aa')}\,\underset{\underset{A\cap B'}{\cap}}{c'} \in A'(A\cap B')$. Thus the kernel of f is as claimed.

The final key to the Jordan-Hölder theorem is the following:

<u>Theorem</u>: Any two subnormal (resp. normal) series of a group G have subnormal (resp. normal) refinements that are equivalent.

<u>Proof</u>: Let G be a group, and start with two subnormal series, the case of normal series being more or less identical. Say $G = G_0 \geq G_1 \geq \cdots \geq G_n$ and $G = H_0 \geq H_1 \geq \cdots \geq H_m$, and set $G_{n+1} = H_{m+1} = \{id\}$. Now between the groups G_i and G_{i+1}, we can identify a number of subgroups:

$$G_i = G_{i+1}(G_i \cap H_0) \geq G_{i+1}(G_i \cap H_1) \geq \cdots \geq G_{i+1}(G_i \cap H_j) \geq \cdots$$

$$\geq G_{i+1}(G_i \cap H_{j+1}) \geq \cdots \geq G_{i+1}(G_i \cap H_{m+1}) = G_{i+1}.$$

To simplify notation, rename these groups as

$$G_i = G_{i,0} \geq G_{i,1} \geq G_{i,2} \geq \cdots \geq G_{i,j} \geq \cdots \geq G_{i,m} \geq G_{i,m+1}$$

This is our refinement of the original series $G_0 \geq G_1 \geq \cdots \geq G_n$:

$$G = G_{0,0} \geq G_{0,1} \geq \cdots \geq G_{0,m} \geq G_{0,m+1} = G_{1,0} \geq G_{1,1} \geq \cdots \text{ etc} \ldots$$

$$\geq G_{n-1,m} \geq G_{n-1,m+1} = G_{n,0} \geq \cdots \geq G_{n,m}.$$

Of course this is not a subnormal series unless we have normality of each successive group in the previous one. Applying the Zassenhaus lemma to $G_{i+1} \trianglelefteq G_i$ and $H_{j+1} \trianglelefteq H_j$ exactly gives what we need:

$$G_{i,j+1} = G_{i+1}(G_i \cap H_{j+1}) \trianglelefteq G_{i+1}(G_i \cap H_j) = G_{i,j}$$

So in the end, our refinement of the original series yields a new series with $(n+1)(m+1)$ terms, not necessarily distinct.

Now similarly refine the other series, to get

$$G = H_{0,0} \geq H_{1,0} \geq \cdots \geq H_{n,0} \geq H_{n+1,0} = H_{0,1} \geq H_{1,1} \geq H_{2,1} \geq \cdots$$
$$\geq H_{n,m-1} \geq H_{n+1,m-1} = H_{0,m} \geq \cdots \geq H_{n,m}$$

where this time we've chosen

$$H_{i,j} = H_{j+1}(H_j \cap G_i)$$

and the Zassenhaus lemma applied to $G_{i+1} \trianglelefteq G_i$ and $H_{j+1} \trianglelefteq H_j$ gives

$$H_{i+1,j} = H_{j+1}(H_j \cap G_{i+1}) \trianglelefteq H_{j+1}(H_j \cap G_i) = H_{i,j} .$$

Again, we have $(n+1)(m+1)$ not necessarily distinct terms.

Finally, part (iii) of the Zassenhaus lemma applied to $G_{i+1} \trianglelefteq G_i$, $H_{j+1} \trianglelefteq H_j$ for $0 \leq i \leq n$ and $0 \leq j \leq m$ gives

$$G_{i,j} / G_{i,j+1} = \frac{G_{i+1}(G_i \cap H_j)}{G_{i+1}(G_i \cap H_{j+1})} \simeq \frac{H_{j+1}(G_i \cap H_j)}{H_{j+1}(G_{i+1} \cap H_j)} = H_{i,j} / H_{i+1,j}$$

Thus the two refinements yield equivalent series.

Theorem (Jordan-Hölder)

Any two composition series of a group G are equivalent.

Proof: Since composition series are subnormal series, two composition series S and T of a group G must have equivalent refinements. However every refinement of a composition series is equivalent to the original series, so S and T are equivalent.

Remarks: • This means every group having a composition series determines a unique finite list of simple groups.

• Every finite group has a composition series, so every finite group determines a unique finite list of finite simple groups. Hence the effort to classify finite simple groups:

Theorem: Every finite simple group is isomorphic to one of the following:

- a cyclic group of prime order
- the alternating group A_n, $n \geq 5$
- a group of Lie type, (not to be confused with a Lie group) which means it appears in one of several infinite families of groups
- One of the 26 "sporadic groups".
- The Tits group (or the 27^{th} "sporadic group")

The proof is tens of thousands of pages. When the Hungerford text was published, it was believed that the problem had been solved in 1983 by Gorenstein. This proved to be false (there was a gap) which was filled by Aschbacher and Smith in 2004. Their paper which filled the gap was 1221 pages.

Example: We use the fact (already mentioned):

Finite abelian groups are simple if and only if they are of prime order.

Now use this and apply the Jordan-Hölder theorem to the group $\mathbb{Z}_n$. Since $\mathbb{Z}_n$ is finite it has a composition series,

$$\mathbb{Z}_n = G_0 \geq G_1 \geq \cdots \geq G_n \geq \{id\}$$

and since each quotient G_i/G_{i+1} must be cyclic of prime order, it's of the form

$$\mathbb{Z}_n = \mathbb{Z}_{p_1 p_2 \cdots p_n} \geq \mathbb{Z}_{p_1 p_2 \cdots p_{n-1}} \geq \cdots \geq \mathbb{Z}_{p_1} \geq \{id\}.$$

where $p_1, \ldots, p_n$ are primes (not necessarily distinct) with $n = p_1 p_2 \cdots p_n$.

If $n = q_1 \cdots q_m$ is any other factorization into primes, then

$$\mathbb{Z}_n = \mathbb{Z}_{q_1 \cdots q_m} \geq \mathbb{Z}_{q_1 \cdots q_{m-1}} \geq \cdots \geq \mathbb{Z}_{q_1} \geq \{id\}$$

is another composition series of $\mathbb{Z}_n$, which must be equivalent to the original composition series by

Jordan-Hölder. But the factors in each case are $\{\mathbb{Z}_{p_1}, \mathbb{Z}_{p_2}, \ldots, \mathbb{Z}_{p_n}\}$ and $\{\mathbb{Z}_{q_1}, \mathbb{Z}_{q_2}, \ldots, \mathbb{Z}_{q_m}\}$, and so up to permutation the lists $\{p_1, \ldots, p_n\}$ and $\{q_1, \ldots, q_m\}$ are the same. I.e. every integer n admits a unique prime factorization.

<u>Example</u>: Since A_n, $n \geq 5$ is a simple group, the series $S_n \geq A_n \geq \{id\}$ is a composition series.

If N were some other proper, nontrivial subgroups of S_n, it must satisfy either:

$$|S_n : N| = |S_n : A_n| = 2$$
$$\text{or } |S_n : N| = |A_n : \{id\}| = n!/2,$$

since $S_n \geq N \geq \{id\}$ is a subnormal series and thus admits a refinement to a composition series that is equivalent to $S_n \geq A_n \geq \{id\}$, by Jordan-Holder.

However $|S_n : N| = n!/2$ is impossible since:

<u>Lemma</u>: If G is a group and $H, K \leq G$ with $|G:H|$ and $|G:K|$ finite, then say $|G:H| = n$ and $|G:K| = m$. We have

$$\operatorname{lcm}(n, m) \leq |G : H \cap K| \leq nm.$$

and so

$$|S_n : A_n \cap N| \geq \operatorname{lcm}(n!/2, 2) \geq \frac{n!}{2} \quad (\text{since } n \geq 5).$$

In particular, $A_n \cap N$ is a nontrivial normal subgroup of A_n, a contradiction. On the other hand, if $|S_n : N| = 2$ then it is easy to argue that $N = A_n$.

<u>Conclusion</u>: A_n is the only proper, nontrivial normal subgroup of S_n.