Now if $|G| = p^n$, then note that since

$$|G| = |G : C(x)| \cdot |C(x)|,$$

the terms $|G : C(x)|$ must all be divisible by p. So we have; from the class equation:

$$p^n = |C(G)| + \text{divisible by } p$$

$$\Longrightarrow |C(G)| \text{ is divisible by } p \text{, so it's nontrivial.}$$

So now when we take $G/_{C(G)}$, we get another p-group (again its order is p^m for some m). If $m > 0$ then its centre is nontrivial again, giving a ~~nontrivial~~ proper $C_2(G) \subset G$. Then $G/_{C_2(G)}$ is also a p-group. if it's trivial, stop, because that means $G = C_2(G)$ is nilpotent. Otherwise $C(G/_{C_2(G)})$ is nontrivial, and we get a proper $C_3(G) \subset G \ldots$

because G is finite, this process must terminate, so eventually $C_k(G) = G$ and G is nilpotent.

<u>Theorem</u>: If G and H are nilpotent then so is $G \times H$.

<u>Proof</u>: First we note that

$$C(G \times H) = C(G) \times C(H) \quad \text{(this is an easy check)}.$$

We want to show by induction that $C_i(G\times H) = C_i(G)\times C_i(H)$, so with the base case done we assume $C_{i-1}(G\times H) = C_{i-1}(G)\times C_{i-1}(H)$ and proceed as follows:

First we check that the quotient map $G\times H \longrightarrow G\times H / C_{i-1}(G\times H)$ is the composition:

$$G\times H \xrightarrow{\pi=(\pi_G,\,\pi_H)} G/C_{i-1}(G)\times H/C_{i-1}(H) \xrightarrow[\sim]{\psi} \frac{G\times H}{\underbrace{C_{i-1}(G)\times C_{i-1}(H)}_{N}}$$

$$(g,h)\longmapsto \left(gC_{i-1}(G),\, hC_{i-1}(H)\right) \longmapsto ((g,h)N)$$

$$= \frac{G\times H}{\underbrace{C_{i-1}(G\times H)}_{N}}$$

So then

$$C_i(G\times H) = \pi^{-1}\psi^{-1}\left(C\left(\frac{G\times H}{C_{i-1}(G\times H)}\right)\right)$$

$$= \pi^{-1}\left(C\left(G/C_{i-1}(G)\times H/C_{i-1}(H)\right)\right)$$

check that ψ^{-1} works this way

$$= \pi^{-1}\left(C\left(G/C_{i-1}(G)\right)\times C\left(H/C_{i-1}(H)\right)\right)$$

$$= \pi_G^{-1}\left(C\left(G/C_{i-1}(G)\right)\right)\times \pi_H^{-1}\left(C\left(H/C_{i-1}(H)\right)\right)$$

$$= C_i(G)\times C_i(H).$$

So, by induction our claim holds. Now choose n large enough that $C_n(G) = G$ and $C_n(H) = H$. Then $C_n(G \times H) = C_n(G) \times C_n(H) = G \times H$, so $G \times H$ is nilpotent.

Surprisingly, we can characterize finite nilpotent groups in terms of their Sylow subgroups. Using the previous theorem is key.

Theorem: A finite group is nilpotent if and only if it is isomorphic to the direct product of its Sylow subgroups.

For this proof, we need a lemma:

Lemma: Suppose G is nilpotent and $H \leq G$ is a proper subgroup. The normalizer of H in G is

$$N_G(H) = \{x \in G \mid xNx^{-1} = N\}$$

be it is "the largest subgroup K of G such that H is normal in K". Obviously $H \leq N_G(H)$.

Then H is a proper subgroup of $N_G(H)$.

Proof of Lemma:

Begin with $C_0(G) = \{e\}$, then $C_1(G) = C(G)$, ... etc. Let n be the largest integer such that $C_n(G) \leq H$, such an n exists since H is a proper subgroup and $\exists\, n$ s.t. $C_n(G) = G$ by nilpotency.

Now choose $a \in C_{n+1}(G) \setminus H$. Now since $a \in C_{n+1}(G)$, $aC_n(G)$ is in the centre of $G/C_n(G)$.

Writing C_n in place of $C_n(G)$, we then have for all $h \in H$:

$$haC_n = (hC_n)(aC_n) = (aC_n)(hC_n) = ahC_n.$$ Thus $ha = ahh'$ for some $h' \in C_n \subseteq H$. Thus $a^{-1}ha = hh'$ for every $h \in H$, meaning $a^{-1}Ha = H$. Thus $a^{-1} \in N_G(H)$ but $a^{-1} \notin H$, so $H \subset N_G(H)$ is proper.

Proof of Theorem:

First note that if G is a direct product of its Sylow subgroups, then it is nilpotent. This is because for every prime p with $p^n \mid |G|$, the Sylow p-subgroup is of order p^n, hence nilpotent, and therefore the product of such groups is also nilpotent.

Now we prove the converse. Suppose G is nilpotent and finite, and $P \subset G$ is a Sylow p-subgroup of G. If $P = G$ we're done. If $P \subset G$ is proper, then P is also a proper subgroup of $N_G(P)$, by our lemma. For Sylow p-subgroups it is not hard to check that $N_G(N_G(P)) = N_G(P)$, which by our lemma actually forces $N_G(P) = G$. Thus P is normal in G, and is therefore the unique Sylow p-subgroup of G

for this particular prime p.

So, suppose $|G| = p_1^{n_1} \cdots p_k^{n_k}$ and for each p_i let P_i be the corresponding unique Sylow p-subgroup with $|P_i| = p_i^{n_i}$. Then $P_i \cap P_j = \{e\}$ for all i, j with $i \neq j$ since $|P_i|$ and $|P_j|$ have no common factors.

Thus $\forall x \in P_i$ and $y \in P_j$, $xy = yx$.

Therefore if we consider an element of $P_1 P_2 \cdots P_{i-1} P_{i+1} \cdots P_k$, we see that its order must divide $p_1^{n_1} \cdots p_{i-1}^{n_{i-1}} p_{i+1}^{n_{i+1}} \cdots p_k^{n_k}$.

(Since $a_1 \cdots a_{i-1} a_{i+1} \cdots a_k \in P_1 \cdots P_{i-1} P_{i+1} \cdots P_k$ implies $(a_1 \cdots a_{i-1} a_{i+1} \cdots a_k)^l = a_1^l \cdots a_{i-1}^l a_{i+1}^l \cdots a_k^l$, so if this were the identity then l would divide $p_j^{n_j}$, for $j \neq i$).

Therefore $P_i \cap (P_1 \cdots P_{i-1} P_{i+1} \cdots P_k) = \{e\}$ since their orders share no common factor and

$P_1 P_2 \cdots P_k = P_1 \times \ldots \times P_k$ since every element is uniquely written as $\prod_{i=1}^{k} a_i^{m_i}$ for some $a_i \in P_i$ and $m_i \mid p_i^{n_i}$.

Now since
$$|G| = p_1^{n_1} \cdots p_k^{n_k} = |P_1 \times \ldots \times P_k| = |P_1 \cdots P_k| \text{ and}$$

$P_1 \cdots P_k \subset G$, we must have
$$G = P_1 \cdots P_k \simeq P_1 \times \ldots \times P_k.$$

We can produce a new sequence of normal subgroups of a group G, allowing for another useful decomposition of G as follows.

Definition: If $a, b \in G$, the element $aba^{-1}b^{-1}$ is called a commutator and is denoted $[a,b]$. The subgroup of G generated by $\{[a,b] \mid a, b \in G\}$ is denoted G' and is called the commutator subgroup.

Remarks: • $[a,b] \in G$ can be thought of as "how far a, b are from commuting"

• $G' = \{e\}$ if and only if G is abelian, so G' can be thought of as a measure of how far G is from being abelian.

Theorem: Let G be a group. Then $G' \trianglelefteq G$ and G/G' is abelian. Moreover, if $N \trianglelefteq G$ is any other normal subgroup, then G/N is abelian if and only if $N \supseteq G'$.

Proof: First, we prove G' is normal. To see this, let

$$S = \{aba^{-1}b^{-1} \mid a, b \in G\}$$

denote the generating set of G'.

Now given $g \in G$, consider gSg^{-1}:

$$gSg^{-1} = \{gaba^{-1}b^{-1}g^{-1} \mid a, b \in G\}$$
$$= \{(gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} \mid a, b \in G\}$$
$$= \{aba^{-1}b^{-1} \mid a, b \in G\} \quad ?$$

since $a \mapsto gag^{-1}$ is a bijection $G \to G$

$$= S.$$

Thus since $G' = \langle S \rangle$ and $gSg^{-1} = S$ we know that $gG'g^{-1} = \langle gSg^{-1} \rangle = \langle S \rangle = G'$, so G' is normal.

To see that G/G' is abelian, let $aG', bG' \in G/G'$ be given. Then $aba^{-1}b^{-1}G' = G' \Rightarrow (abG')(a^{-1}b^{-1}G') = G'$, so

$$(aG')(bG')(a^{-1}G')(b^{-1}G') = G'$$
$$\Rightarrow (aG')(bG') = (bG')(aG').$$

Last, let $N \subset G$ be normal and suppose G/N is abelian. Then $abN = baN$ for all $a, b \in G$

$$\Rightarrow aba^{-1}b^{-1}N = N, \text{ so } aba^{-1}b^{-1} \in N \ \forall a, b \in G,$$

so $S \subset N$ and thus $G' = \langle S \rangle \subset N$. On the other hand if $G' \subset N$ it is easy to see that G/N is abelian, because there is an onto homomorphism:

$$G/G' \longrightarrow G/N.$$

<u>Definition</u>: Given a group G, set $G^{(1)} = G'$, and in general for $i \geq 2$ set $G^{(i)} = (G^{(i-1)})'$. The group $G^{(i)}$ is the i^{th} <u>derived subgroup</u> of G and the sequence of subgroups $G \geq G^{(1)} \geq G^{(2)} \geq \dots$ is called the <u>derived</u> <u>series</u> of G.

<u>Definition</u>: If $\exists n$ such that $G^{(n)} = \{id\}$ then G is called <u>solvable</u>.

<u>Proposition</u>: Nilpotent groups are solvable.

Proof: By definition of $C_i(G)$, we can compute:

The quotient homomorphism $q_i : G \longrightarrow G/C_{i-1}(G)$ gives, upon restriction to $C_i(G)$ an onto homomorphism $h: C_i(G) \longrightarrow C\left(G/C_{i-1}(G)\right)$. The kernel of h is exactly $C_{i-1}(G)$ because h is the restriction of the quotient q_i, so the first isomorphism theorem gives

$$C_i(G)/C_{i-1}(G) \cong C\left(G/C_{i-1}(G)\right),$$ which is abelian.

Thus $C_i(G)' \subset C_{i-1}(G)$ for all $i > 1$, and
$$C_1(G)' = C(G)' = \{e\},$$

since $C(G)$ is abelian.

Now because G is nilpotent, $\exists n$ such that $G = C_n(G)$.

Thus $C\left(G/C_{n-1}(G)\right) = C_n(G)/C_{n-1}(G) = G/C_{n-1}(G)$ and we

conclude that $G/C_{n-1}(G)$ is abelian; therefore

$G' \subset C_{n-1}(G)$. Then we find

$G^{(2)} = (G^{(1)})' \subset C_{n-1}(G)' \subset C_{n-2}(G)$, and therefore

$G^{(3)} = (G^{(2)})' \subset C_{n-2}(G)' \subset C_{n-3}(G)$, etc, and in

the end we get $G^{(n)} \subset C_{n-n}(G) = C_0(G) = \{e\}$,

so that G is solvable.

As with nilpotent groups, solvable groups behave well with respect to quotients and subgroups.

<u>Theorem</u>: Suppose G is a solvable group.

(i) Every subgroup of G is solvable.

(ii) Every quotient of G is solvable.

(iii) If N is a normal subgroup of G and both N and G/N are solvable, then so is G.

<u>Proofs</u>: (i) Suppose $f: G \longrightarrow H$ is an onto homomorphism. Then it is not hard to verify that $f(G^{(i)}) = H^{(i)}$, since every homomorphism maps commutators to commutators:

$$f(aba^{-1}b^{-1}) = f(a)f(b)f(a)^{-1}f(b)^{-1}.$$

Thus if $G^{(n)} = \{id\}$ then $H^{(n)} = f(\{id\}) = \{id\}$, so H is solvable. The proof of (ii) is similar.

To prove (iii), note that if G/N is solvable then the quotient $q: G \longrightarrow G/N$ gives

$$q(G^{(n)}) = (G/N)^{(n)} = \{id\} \text{ for some } n \geq 1,$$

meaning $G^{(n)} \subseteq \ker q = N$. But N is assumed solvable, so $G^{(n)} \subset N$ implies $G^{(n)}$ is solvable. Thus $(G^{(n)})^{(k)} = G^{(n+k)}$ is the identity for some k. Thus G is solvable.

<u>Example</u>: The alternating groups $A_n \subset S_n$ for $n \geq 5$ are simple. They're also nonabelian, so A_n for $n \geq 5$ is not solvable.

$\Longrightarrow S_n$ is not solvable for $n \geq 5$.

Solvability is a powerful restriction on groups. It allows for (for example) the strengthening of many existing structure theorems if we restrict our attention to solvable groups only. Here is a strengthening of Sylow's theorems:

<u>Theorem</u> (Hall). Let G be a solvable group of order mn, with $\gcd(m,n)=1$. Then:

(i) G contains a subgroup of order m

(ii) Any two subgroups of G of order m are conjugate

(iii) Any subgroup of G of order k where $k \mid m$ is contained in a subgroup of order m.

We will not prove this generalization, but simply mention it to highlight the strength of the solvability condition.

§2.8 Normal and Subnormal series.

Our goal here is to repeat a portion of material from Algebra 2 in a more general setting, culminating in a proof of the Jordan-Hölder theorem.

In Algebra 2, you saw this theorem in the special case of finite groups — where the proof is much simpler. The core ideas here are significantly harder (and carry the names of famous mathematicians as a result).

Definition: A subnormal series of a group G is a chain of subgroups

$$G = G_0 > G_1 > \cdots > G_n$$

such that G_{k+1} is normal in G_k for all $k = 0, \dots, n-1$. The <u>factors</u> of the series are the quotients G_k/G_{k+1}, and the <u>length</u> of the series is the number of nontrivial factors. A subnormal series in which each G_i is additionally normal in G is called <u>normal</u>.

<u>Examples</u>: The derived series

$$G > G^{(1)} > \cdots > G^{(n)}$$

is a normal series (fact that needs checking: $G^{(i)} \trianglelefteq G \; \forall i$

The ascending central series

$$G = C_n(G) > C_{n-1}(G) > \cdots > C_1(G)$$

is a normal series if <u>G is nilpotent</u>. If G is <u>not</u> nilpotent then it can fail to be even a subnormal series.

Definition Let $G = G_0 > G_1 > \cdots > G_n$ be a subnormal series. A <u>one-step-refinement</u> of this series is

$$G = G_0 > G_1 > \cdots > G_i > N > G_{i+1} > \cdots > G_n$$

where $N \trianglelefteq G_i$ and $G_{i+1} \trianglelefteq N$, or

$$G = G_0 > G_1 > \cdots > G_n > N$$

where $N \trianglelefteq G_n$.

A refinement of a subnormal series S is any subnormal series obtained from S by a finite number of one-step refinements. A refinement is <u>proper</u> if its length is greater than the length of the initial series.

<u>Definition</u>: A subnormal series $G = G_0 > \cdots > G_n = \langle id \rangle$ is a <u>composition series</u> if each factor G_i/G_{i+1} is simple. A subnormal series $G = G_0 > \cdots > G_n = \langle id \rangle$ is a <u>solvable series</u> if each factor G_i/G_{i+1} is abelian...