Nilpotent and solvable groups

written by Night Shift in Math on Functor Network
original link: https://functor.network/user/854/entry/375

Definition 1. *Let G be a group, $C_1(G) = C(G)$, and define $C_i(G)$ to be the inverse image of $C(G/C_{i-1}(G))$ under the canonical projection $G \to G/C_{i-1}(G)$. The ascending central series of G is*

$$\langle e \rangle \leq C_1(G) \leq C_2(G) \leq \cdots$$

G is said to be nilpotent iff $\exists n \in \mathbb{N}, C_n(G) = G$.

Theorem 1. *Every finite p-group is nilpotent.*

Proof. G and all its nontrivial quotients are p-groups and thus have nontrivial centers. Thus if $G \neq C_i(G)$, $C_i(G) < C_{i+1}(G)$. Since G is finite, $\exists n \in \mathbb{N}, C_n(G) = G$. □

Theorem 2. *The direct product of a finite number of nilpotent groups is nilpotent.*

Proof. Suppose $G = H \times K$. Assume that $C_i(G) = C_i(H) \times C_i(K)$. Let $\pi_H : H \to H/C_i(H)$ be the canonical epimorphism. Similarly for π_K. Verify that the canonical epimorphism $\phi : G \to G/C_i(G)$ is the composition

$$G = H \times K \xrightarrow{\pi} H/C_i(H) \times K/C_i(K) \xrightarrow{\psi} (H \times K)/(C_i(H) \times C_i(K)) = G/C_i(G)$$

where $\pi = \pi_H \times \pi_K$ and ψ is an isomorphism. Consequently,

$$\begin{aligned} C_{i+1}(G) &= \phi^{-1}[C(G/C_i(G))] = \pi^{-1} \circ \psi^{-1}[C(G/C_i(G))] \\ &= \pi^{-1}[C(H/C_i(H)) \times C(K/C_i(K))] \\ &= \pi_H^{-1}[C(H/C_i(H))] \times \pi_K^{-1}[C(K/C_i(K))] \\ &= C_{i+1}(H) \times C_{i+1}(K) \end{aligned}$$

The inductive step is proved so $C_i(G) = C_i(H) \times C_i(K)$ for all i. Since H, K are nilpotent, $\exists n \in \mathbb{N}$, $C_n(H) = H, C_n(K) = K$. Thus $C_n(G) = G$. □

Lemma 1. *If H is a proper subgroup of a nilpotent group G, then H is a proper subgroup of its normalizer $N_G(H)$.*

Proof. Let $C_0(G) = \langle e \rangle$ and let n be the largest index such that $C_n(G) \leq H$. Choose $a \in C_{n+1}(G) \setminus H$. $\forall h \in H, ahC_n(G) = haC_n(G)$. Thus $\exists h' \in C_n(G), ah = hah'$. This implies $a \in N_G(H)$. Thus $a \in N_G(H) \setminus H$. □

Proposition 1. *A finite group is nilpotent iff it is the direct product of its Sylow subgroups.*

Proof. If G is the direct product of its Sylow p-subgroups, then it is nilpotent by our previous results. If G is nilpotent and P is a Sylow p-subgroup of G for some prime p, then either $G = P$ or P is a proper subgroup. In the latter case, P is a proper subgroup of $N_G(P)$. Since $N_G(N_G(P)) = N_G(P)$, $N_G(P) = G$. Thus $P \lhd G$ and hence the unique Sylow p-subgroup of G. Let $|G| = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ where p_i are distinct primes and let $P_1, P_2, \cdots, P_k$ be the corresponding proper normal Sylow subgroups of G. For $i \neq j$, $P_i \cap P_j = \langle e \rangle$. Thus for any $x \in P_i, y \in P_j$, $xy = yx$. It is easy to see that $G = P_1 P_2 \cdots P_k$ is an inner direct product. □

Corollary 1. *If G is a finite nilpotent group and $m \mid |G|$, G has a subgroup of order m.*

Definition 2. *Let G be a group. The subgroup generated by $\{aba^{-1}b^{-1} \mid a, b \in G\}$ is called the commutator subgroup of G and is denoted G'. The elements $[a, b] = aba^{-1}b^{-1}$ are called commutators.*

G is abelian iff $G' = \langle e \rangle$.

Theorem 3. *If G is a group, then $G' \trianglelefteq G$ and G/G' is abelian. If $N \trianglelefteq G$, then G/N is abelian iff $G' \leq N$.*

Proof. Note that for every endomorphism $f : G \to G$, $f(G') \leq G'$. Hence, $G' \trianglelefteq G$. Since $(ab)(ba)^{-1} \in G', abG = baG$ and hence G/G' is abelian. If G/N is abelian, $abN = baN$ for all $a, b \in G$, whence $ab(ba)^{-1} \in N$. Therefore $G' \leq N$. If $G' \leq N, ab(ba)^{-1} \in N$ so $abN = baN$. □

Definition 3. *Let G be a group and $G^{(1)} = G'$. Define $G^{(i)} = (G^{(i-1)})'$. $G^{(i)}$ is called the ith derived subgroup of G. The derived series of G is $G \geq G^{(1)} \geq G^{(2)} \geq \cdots$. A group G is said to be solvable iff $G^{(n)} = \langle e \rangle$ for some n.*

Proposition 2. *Every nilpotent group is solvable.*

Proof. By definition, $C_i(G)/C_{i-1}(G) = C(G/C_{i-1}(G))$ is abelian. $C_i(G)' \leq C_{i-1}(G)$ and $C(G)' = \langle e \rangle$. For some n, $G = C_n(G)$. Therefore $C(G/C_{n-1}(G)) = G/C_{n-1}(G)$ is abelian and hence $G' \leq C_{n-1}(G)$. $G^{(2)} \leq C_{n-1}(G)' \leq C_{n-2}(G)$. Continuing, $G^{(n)} \leq C(G)' = \langle e \rangle$. Hence G is solvable. □

Theorem 4. *(i) Every subgroup and every homomorphic image of a solvable group is solvable.*

(ii) If N is a normal subgroup of a group G such that N and G/N are solvable, then G is solvable.

Proof. (i) If $f : G \to H$ is a homomorphism [resp. epimorphism] then $f(G^{(i)}) \leq H^{(i)}$ [resp. $f(G^{(i)}) = H^{(i)}$] for all i. Suppose f is an epimorphism and G is solvable. For some n, $\langle e \rangle = f(G^{(n)}) = H^{(n)}$, whence H is solvable. Similarly for the subgroup.

(ii) Let $f : G \to G/N$ be the canonical epimorphism. $\exists n \in \mathbb{N}, f(G^{(n)}) = (G/N)^{(n)} = \langle e \rangle$. Hence $G^{(n)} \leq \ker f = N$. By (i), $G^{(n)}$ is solvable. Hence $\exists k \in \mathbb{N}, G^{(n+k)} = (G^{(n)})^{(k)} = \langle e \rangle$. □

Corollary 2. *If $n \geq 5$, the symmetric group S_n is not solvable.*

Proof. Since A_n is nonabelian, A_n' is not trivial. Since $A_n' \trianglelefteq A_n$ and A_n is simple, $A_n' = A_n$. Thus $A_n^{(i)} = A_n \neq \{(1)\}$ for all i whence A_n is not solvable. Thus S_n is not solvable. □

Definition 4. *A subgroup H of a group G is said to be characteristic iff $\forall f \in \operatorname{Aut} G, f(H) \leq H$. It is fully invariant iff for every endomorphism $f : G \to G$, $f(H) \leq H$. A minimal subgroup of a group G is a nontrivial normal subgroup that contains no proper subgroup which is normal in G.*

Lemma 2. *Let N be a normal subgroup of a finite group G and H any subgroup of G.*

(i) If H is a characteristic subgroup of N, then $H \trianglelefteq G$.

(ii) Every normal Sylow p-subgroup of G is fully invariant.

(iii) If G is solvable and N is a minimal normal subgroup, then N is an abelian p-group for some prime p.

Proof. (i) Since $\forall a \in G, aNa^{-1} = N$, conjugation by a is an automorphism of N. Since H is characteristic in N, $aHa^{-1} \leq H$ for all $a \in G$. Hence $H \trianglelefteq G$.

(ii) Let P be a normal Sylow p-subgroup of G. Then $P = G(p)$. Let $f : G \to G$ be an endomorphism. For $g \in f(P)$, $\exists h \in P, g = f(h)$. Suppose $|h| = p^k$. Then $g^{p^k} = e$ so $|g| \mid p^k$ implying $g \in P$. Thus $f(P) \leq P$.

(iii) It is easy to see that N' is fully invariant in N. Whence $N' \trianglelefteq G$. Thus $N' = \langle e \rangle$ or $N' = N$. Since N is solvable, $N' = \langle e \rangle$ and N is a nontrivial abelian group. Let P be a nontrivial Sylow p-subgroup of N for some prime p. Since N is abelian, P is normal in N and hence fully-invariant in N. Consequently, $P \trianglelefteq G$. Since N is minimal and P is nontrivial, $P = N$. □

Theorem 5 (Hall)**.** *Let G be a finite solvable group of order mn with $(m, n) = 1$. Then*

(i) G contains a subgroup of order m.

(ii) Any two subgroups 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.

Proof. The proof proceeds by induction on $|G|$, with orders less than or equal to 5 being trivial. There are two cases:

1. There is a nontrivial proper normal subgroup H of G whose order is not divisible by n.

2. Every proper nontrivial normal subgroup of G has order divisible by n.

Case 1. (i) $|H| = m_1n_1, m_1 \mid m, n_1 \mid n, n_1 < n$. G/H is a solvable group of order $\frac{mn}{m_1n_1} < mn$ with $(m/m_1, n/n_1) = 1$. By induction, G/H contains a subgroup A/H of order m/m_1 where $A \leq G$. Then $|A| = |H|[A : H] = mn_1 < mn$. A is solvable and contains a subgroup of order m.

(ii) Suppose B, C are subgroups of G of order m. Since $H \trianglelefteq G$, HB is a subgroup whose order k necessarily divides mn. $k = |HB| = \frac{|H||B|}{|H\cap B|} = \frac{m_1n_1m}{|H\cap B|}$ whence $k \mid m_1n_1m$. Since $(n, m_1) = 1$, $k \mid mn_1$. By Lagrange's theorem, $m \mid k$ and $m_1n_1 \mid k$. Thus $(m, n) = 1$ implies $mn_1 \mid k$. Therefore $k = mn_1$. Similarly, $|HC| = mn_1$. Thus HB/H and HC/H are subgroups of G/H of order m/m_1. By induction, they are conjugate for some $xH \in G/H$. $xH(HB/H)x^{-1}H = HC/H$. Thus $xHBx^{-1} = HC$. xBx^{-1} and C are subgroups of HC of order m and are therefore conjugate in HC by induction. Hence B is conjugate to C in G.

(iii) If a subgroup K of G has order $k \mid m$, then $HK/H \cong K/H \cap K$ has order dividing k. Since $HK/H \leq G/H$, $|HK/H| \mid \frac{mn}{m_1n_1}$. $(k, n) = 1$ implies $|HK/H| \mid \frac{m}{m_1}$. By induction, there is a subgroup A/H of G/H of order $\frac{m}{m_1}$ containing HK/H. Clearly $K \leq A$. Since $|A| = |H||A/H| = mn_1 < mn$, K is contained in a subgroup of A of order m by induction.

Case 2. If H is a minimal normal subgroup, then $|H| = p^r$ for some prime p. Since $(m, n) = 1$ and $n \mid |H|$, $n = p^r$ and H is a Sylow p-subgroup of G. H is the only minimal subgroup of G. Every nontrivial normal subgroup of G contains H.

(i) Let K be a normal subgroup of G such that K/H is a minimal normal subgroup of G/H. $|K/H| = q^s$ for some prime q where $q \neq p$. $|K| = p^rq^s$. Let S be a Sylow q-subgroup of K and $M = N_G(S)$. We shall show $|M| = m$. Since $H \trianglelefteq K$, $HS \leq K$. Clearly $H \cap S = \langle e\rangle$ so that $|HS| = |K|$ whence $HS = K$. Since $K \trianglelefteq G, S \leq K$, every conjugate of S in G lies in K. Since S is a Sylow subgroup of K, all these subgroups are conjugate in K. Let $N = N_K(S)$. Let c be the number of conjugates of S in G. Since $S \leq N \leq K, K = HN$, and

$$c = [G : M] = [K : N] = [HN : N] = [H : H \cap N]$$

We shall show that $H \cap N = \langle e\rangle$ so that $c = |H| = p^r$ and hence $|M| = m$. We first show $H \cap N \leq C(K)$ then show $C(K) = \langle e\rangle$. Let $x \in H \cap N$ and $k \in K$. Since $K = HS, \exists h \in H, s \in S, k = hs$. Since H is abelian, we only need to show $xs = sx$. $(xsx^{-1})s^{-1} \in S$ since $x \in N$. But $x(sx^{-1}s^{-1}) \in H$. Thus $xsx^{-1}s^{-1} \in H \cap S = \langle e\rangle$. It is easy to see that $C(K)$ is a characteristic subgroup of K. Since $K \trianglelefteq G, C(K) \trianglelefteq G$. If $C(K) \neq \langle e\rangle$, then $H \leq C(K)$. This with $K = HS$ implies $S \trianglelefteq K$. S is a normal Sylow p-subgroup of K and is thus fully invariant in K, and hence normal in G. This implies $H \leq S$, a contradiction. Thus $C(K) = \langle e\rangle$.

(ii) Let M be as in (i) and suppose B is a subgroup of G of order m. Note $m \mid |BK|$ and $p^rq^s \mid |BK|$. Since $(m, p) = 1$, $nm \mid |BK|$. Hence $G = BK$. Thus $G/K \cong B/B \cap K$ implying that $|B \cap K| = q^s$. by the second Sylow theorem, $B \cap K$ is conjugate to S in K. Furthermore, $B \cap K$ is normal in B and hence $B \leq N_G(B\cap K)$. Conjugate subgroups have conjugate normalizers. Hence

$N_G(B \cap K)$ and $N_G(S) = M$ are conjugate in G. Thus $|N_G(B \cap K)| = |M| = m$. But $|B| = m$ so $B = N_G(B \cap K)$. Thus B and M are conjugate.

(iii) Let $D \leq G$, where $|D| = k$ and $k \mid m$. Let M and H be as in (i). Then $D \cap H = \langle e \rangle$ and $|DH| = kp^r$. Also, $|G| = mp^r$, $M \cap H = \langle e \rangle$ and $MH = G$. Hence $M(DH) = G$ and $|M \cap DH| = k$. Let $M^* = M \cap DH$ then by applying (ii) to DH, M^* and D are conjugate. $\exists a \in G, aM^*a^{-1} = D$. Since $M^* \leq M$, $D \leq aMa^{-1}$ and $|aMa^{-1}| = m$. □