7. Nilpotent groups and Finite abelian groups

<u>Def</u>: The <u>ascending central series</u> of a group G is

$$1 = Z_0 \leq Z_1 = Z(G) \leq Z_2 \leq Z_3 \leq \cdots$$

where $Z_{i+1}/Z_i = Z(G/Z_i)$. If $Z_n = G$ for some n, then G is <u>nilpotent</u> of <u>class</u> n, where n is minimal s.t. $Z_n = G$.

Think of this process as follows:

* Start with G, find the center $Z(G)$, quotient out by it.
* Now repeat this process (find center & quotient out by it).
* We either get stuck (center is trivial), or eventually reach 1 (quotient was abelian). G is nilpotent when this latter case occurs.

<u>Examples</u>:
- Abelian groups are nilpotent.
- If $n \geq 3$, then $Z(S_n) = 1$ thus S_n is not nilpotent.

<u>Prop 7.1</u>: If $|G| = p^k$, then G is nilpotent.

<u>Pf</u> (sketch): Since $Z(G) > 1$, G/Z_1 is a p-group, so $Z_2/Z_1 = Z(G/Z_1) \neq 1$. Thus $Z_2 \gneq Z_1$. Likewise, if $Z_2 \neq G$, then $Z_3 \gneq Z_2$, and so on.

<u>Prop 7.2</u>: If G is nilpotent, then G is solvable.

<u>Pf</u>: Z_{i+1}/Z_i is abelian (it is $Z(G/Z_i)$), thus

$G = Z_n \geq Z_{n-1} \geq \cdots \geq Z_0$ is a subnormal series with abelian factors. $\square$

Cor: Finite p-groups are solvable.

Note: Cyclic gps $\subsetneq$ abelian gps $\subsetneq$ nilpotent gps $\subsetneq$ solvable gps $\subsetneq$ all gps.

Also, note that $Z_i = \{ x Z_{i-1} : xy Z_{i-1} = yx Z_{i-1} \ \forall y \in G \}$

$$\Rightarrow \boxed{Z_i = \{ x \in G : [x, y] \in Z_{i-1} \ \forall y \in G\}} \qquad (*)$$

Prop 7.3: If G is nilpotent and $H \lneq G$, then $N_G(H) \gneq H$.

Pf: For some i, $Z_i \leq H$, and $Z_{i+1} \not\leq H$.

Claim: $Z_{i+1} \leq N_G(H)$.

Pick $x \in Z_{i+1}$. By $(*)$, $xhx^{-1}h^{-1} \in Z_i < H$ for any $h \in H$.

Thus $xhx^{-1} \in H \ \forall x \in Z_{i+1} \Rightarrow x \in N_G(H)$. $\square$

Cor: If G is nilpotent and $H \lneq G$ maximal, then $H \triangleleft G$.

* The converse holds as well if G is finite (see HW #6).

As a non-example, S_3 is not nilpotent, and $\langle (12) \rangle$ maximal, but $\langle (12) \rangle \ntriangleleft S_3$.

Prop 7.4: If $|G| < \infty$ and $P \leq G$ is p-Sylow, then $N_G(N_G(P)) = N_G(P)$.

Pf: Pick $x \in N_G(N_G(P))$. Then $x N_G(P) x^{-1} \subseteq N_G(P) \Rightarrow xPx^{-1} \subseteq N_G(P)$.

But $P \triangleleft N_G(P)$, thus P is the unique p-Sylow subgp of $N_G(P)$, i.e. $xPx^{-1} = P$. $\square$

Def: If $H, K \leq G$, define $[H, K] = \langle [h,k] : h \in H, k \in K \rangle$.

Note: In the derived series, $G^{(k+1)} = [G^{(k)}, G^{(k)}]$.

Remark: $H \trianglelefteq G$ iff $[G,H] \leq H$.

Prop 7.5: Suppose $K \trianglelefteq G$ and $K \leq H \leq G$. Then $H/K \leq Z(G/K)$ iff $[G,H] \leq K$.

Pf: $[g,h] = g^{-1}h^{-1}gh \in K \ \forall\, g \in G,\ h \in H \iff ghK = hgK \quad \forall g,h$

$\iff H/K \leq Z(G/K)$. □

Def: The descending central series of G is the series

$G = L_0 \geq L_1 \geq L_2 \geq \cdots$, where

$L_1 = [G,G]$, $L_2 = [G, L_1]$, ..., $L_{k+1} = [G, L_k]$.

Note: • $L_k \trianglelefteq G$ for each k.

• By Prop 7.5, $\boxed{L_k/L_{k+1} \leq Z(G/L_{k+1}),\ \text{and}\ Z_k \geq [G, Z_{k+1}]}$

Compare to: $\boxed{Z_{k+1}/Z_k = Z(G/Z_k),\ \text{and}\ L_{k+1} = [G, L_k]}$

Thm 7.6: G is nilpotent iff $L_n(G) = 1$ for some n

Pf: ($\Rightarrow$) Suppose G is nilpotent of class n. Then

$L_1 = [G, L_0] = [G, Z_n] \leq Z_{n-1}$

$L_2 = [G, L_1] \leq [G, Z_{n-1}] \leq Z_{n-2}$

$\vdots$

$L_k = [G, L_{k-1}] \leq [G, Z_{n-k+1}] \leq Z_{n-k}$

Note: The middle inequality follows from $H \leq K \Rightarrow [G,H] \leq [G,K]$.

Since G is nilpotent, $1 = Z_0 \geq L_n$ ✓

($\Leftarrow$) Suppose $L_n = 1$ for some n, and let n be minimal.

$[G, L_{n-1}] = L_n = 1 \implies L_{n-1} \leq Z_1 = Z(G)$. (Prop 7.5).

$[G, L_{n-2}] = L_{n-1} \leq Z_1$. We'll show $L_{n-2} \leq Z_2$, and so on.

Consider $Z_1 \leq L_{n-2} Z_1 \leq G$.

Now, $L_{n-1} = [G, L_{n-2}] \leq [G, L_{n-2} Z_1] \leq Z_1$.

Prop 7.5 $\Rightarrow L_{n-2} Z_1 / Z_1 \leq Z(G/Z_1) = Z_2/Z_1$

Corresp. thm $\Rightarrow L_{n-2} Z_1 = Z_1 \leq Z_2 \implies L_{n-2} \leq Z_2$.

Similarly, $[G, L_{n-3}] = L_{n-2} \leq Z_2 \implies$ (same steps) $L_{n-3} \leq Z_3$

and inductively, $L_{n-k} \leq Z_k$.

By assumption, $G = L_0 \leq Z_n \implies G$ is nilpotent. $\square$.

<u>Prop 7.7</u>: If H & K are nilpotent, then $G = H \times K$ is nilpotent.

<u>Pf</u>: Clearly, $L_0(G) = L_0(H) \times L_0(K)$.

Suppose $L_k(G) = L_k(H) \times L_k(K)$.

Then $L_{k+1}(G) = [H \times K, L_k(H) \times L_k(K)] = [H, L_k(H)] \times [K, L_k(K)]$

$= L_{k-1}(H) \times L_{k-1}(K)$.

If H and K are nilpotent of class m & n, resp, then

$L_N(G) = 1$ if $N \geq m, n$. Thus G is nilpotent. $\square$.

<u>Prop 7.8</u>: A finite gp G is nilpotent iff it is the internal direct product of its Sylow subgps.

<u>Pf</u>: ($\Leftarrow$) Easy.

($\Rightarrow$) Let G be nilpotent and $P \leq G$ be p-Sylow. Then $N_G(N_G(P)) = N_G(P)$, but by Prop 7.3, $N_G(N_G(P)) \gneq N_G(P)$ unless $N_G(P) = G$. Thus, $N_G(P) = G \Rightarrow P \trianglelefteq G$.

Now, let $P_1, \dots, P_n$ be the distinct nontrivial Sylow subgps of G.

(i) $G = P_1 P_2 \cdots P_n$ ✓

(ii) $P_i \trianglelefteq G \quad \forall i$ ✓

(iii) $P_i \cap \langle \cup P_j : j \neq i \rangle = 1$?

If $x \in P_i$, $y \in P_j$, then $xyx^{-1}y^{-1} \in P_i \cap P_j = 1 \Rightarrow xy = yx$.

Now, take $1 \neq x \in P_i$. $|x| \nmid |\langle \cup P_j : j \neq i \rangle|$, so $x \notin \langle \cup P_j : j \neq i \rangle$.

By Thm 6.3, $G \cong P_1 \times P_2 \times \cdots \times P_n$. $\square$

<u>Summary of nilpotent groups</u>

A finite group G is <u>nilpotent</u> if one of the following conditions holds

(i) $Z_n = G$ for some n in the ascending central series

(ii) $L_n = 1$ for some n in the descending central series

(iii) For each $H \lneq G$, $H \lneq N_G(H)$.

(iv) Every Sylow subgp of G is normal

(v) $G \cong P_1 \times \cdots \times P_r$ (its Sylow subgps)

(vi) Every maximal proper subgp is normal (see HW #6).

Finite abelian groups

Thm 7.9: If G is a finite abelian group, then G is a direct sum of cyclic subgps, each of prime power order.

Pf: Since G is abelian, it is nilpotent, thus is the direct sum of its Sylow subgps.

Thus, we may assume that $|G| = p^n$.

Use induction on $|G|$. Base case is trivial.

Pick $a \in G$ of maximal order, say $|a| = p^k$, and choose $H \leq G$ maximal w.r.t. $H \cap \langle a \rangle = 0$.

Set $G_1 = H \oplus \langle a \rangle \leq G$. Claim: $G_1 = G$.

If not, then pick an elt $x + G_1 \in G/G_1$ of order p, i.e., $px \in G_1$.

Say $px = h + ma \in H \oplus \langle a \rangle$.

Since $|x| \leq p^k$, $0 = p^k x = p^{k-1}(px) = p^{k-1}h + p^{k-1}ma \quad (*)$

Note: $p^{k-1}ma \in H \cap \langle a \rangle = 0 \quad$ (b/c $p^{k-1}h \in H$)

But since $|a| = p^k$, $p \mid m$, say $m = pr$. $(r \in \mathbb{Z})$

From $(*)$, we have $p^{k-1}h = p^k x - p^{k-1}ma$

$$\Rightarrow h = px - ma = px - pra = p(x - ra) \in H.$$

But $x \notin G_1 \Rightarrow x - ra \notin H$.

By maximality of H, $(H + \langle x - ra \rangle) \cap \langle a \rangle \neq 0$

So, pick some $h_1 + t(x - ra) = sa \neq 0$ in it,

$$\Rightarrow tx = -h_1 + (s + tr)a \in H \oplus \langle a \rangle = G_1$$

By choice of x, $tx \in G_1 \Rightarrow p \mid t$ (b/c $x+G_1$ has order p in G/G_1).

But we'll now show that this is impossible.

If $p \mid t$, then $t = up$ for some $u \in \mathbb{Z}$.

Now, $sa = h_1 + t(x-ra) = h_1 + up(x-ra) = h_1 + uh \in H \oplus \langle a \rangle = 0$. ↯

Thus, no such $x \in G \setminus G_1$ can exist, so $G = H \oplus \langle a \rangle_r$ and apply IHOP to H. □

<u>Thm 7.10</u>: Suppose G is abelian, $|G| = p^n$ for some prime p, and

$$G = G_1 \oplus G_2 \oplus \cdots \oplus G_r = H_1 \oplus H_2 \oplus \cdots \oplus H_s$$

with each G_i, H_j cyclic and $1 < |G_i| \leq |G_{i+1}|$, $1 < |H_j| \leq |H_{j+1}|$ for all i and j. Then $r = s$ and $G_i \cong H_i$ for $1 \leq i \leq r$.

<u>Pf</u>: Let $H = \{x \in G : px\} = 0$.

Each G_i has a subgp $K_i < G_i$ of order p.

Let $H = K_1 \oplus K_2 \oplus \cdots \oplus K_r$, so $|H| = p^r$.

Similarly, $|H| = p^s \Rightarrow p^r = p^s \Rightarrow r = s$.

Suppose now that k is the min'l index s.t (wlog)

$|H_k| > |G_k| = p^t$.

Then $p^t G = p^t G_{k+1} \oplus \cdots \oplus p^t G_r = p^t H_k \oplus \cdots \oplus p^t H_r$

This contradicts the assumption that there must be the same number of factors.

□

Cor 7.11: (Fundamental Thm of Finite Abelian Groups).

Suppose G is a finite abelian gp, with primes $p_1 < p_2 < \dots < p_k$ dividing $|G|$. Then $G = G_1 \oplus \cdots \oplus G_k$, where G_i is a p_i-group, and $G_i = H_{i,1} \oplus \cdots \oplus H_{i,m_i}$ for each i, with $H_{i,j}$ cyclic and $1 < |H_{i,j}| \leq |H_{i,j+1}|$ for each j.

Pf: Each G_i is a p_i-Sylow subgp, and the second part follows from Theorems 7.9 & 7.10. $\square$

Examples: Below, G is abelian.

(1) Suppose $|G| = 100 = 2^2 \cdot 5^2$. Then $G = G_1 \times G_2$, where G_1 is 2-Sylow and G_2 is 5-Sylow. Then $G_1 \cong \mathbb{Z}_4$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ and $G_2 \cong \mathbb{Z}_{25}$ or $\mathbb{Z}_5 \oplus \mathbb{Z}_5$.

Thus, there are four choices for G up to isomorphism:

$$\mathbb{Z}_4 \oplus \mathbb{Z}_{25}, \quad \mathbb{Z}_4 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5, \quad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{25}, \quad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5.$$

(2) Suppose $|G| = p^4$ for some prime p.

There are five choices for G (up to isom):

$$G \cong \mathbb{Z}_{p^4}, \quad \mathbb{Z}_{p^3} \oplus \mathbb{Z}_p, \quad \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$$

$$\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p, \quad \text{or} \quad \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p.$$