Oct. 20, 2006 (Fri.)

Let G be an abelian group, there there is a natural important homomorphism $m : G \to G$ by $m(x) := mx$ for $m \in \mathbb{N}$. The image is denoted mG and kernel is denoted $G[m]$. Let $G(p) = \{u \in G | o(u) = p^n$ for some $n \geq 0\}$. One can show that $G(p)$ is the Sylow p-subgroup of G. And G is a direct sum of Sylow subgroups. Thus it remains to study finite abelian p-groups. The only non-trivial part of classical theory is showing that a finite abelian p-group is a direct sum of cyclic p-groups.

We also remark that for a given finitely generated abelian group G, the rank, invariant factors, and elementary divisors are unique. To see this, we proceed as following steps:

1. if $\mathbb{Z}^n \cong \mathbb{Z}^m$, then $n = m$.

To see this, let $G \cong \mathbb{Z}^n \cong \mathbb{Z}^m$. We consider $G/2G \cong \mathbb{Z}_2^n \cong \mathbb{Z}_2^m$. Thus $n = m$.

2. let $G_{tor} := \{u \in G | mu = 0$ for some $m\}$. It's clear that $G_{tor} < G$.

3. If

$$G_1 = \mathbb{Z}_{d_1} \oplus ... \oplus \mathbb{Z}_{d_t} \oplus \mathbb{Z}^r,$$
$$\cong G_2 = \mathbb{Z}_{d'_1} \oplus ... \oplus \mathbb{Z}_{d'_{t'}} \oplus \mathbb{Z}^{r'}$$

Then clearly, $G_{1tor} \cong G_{2tor}$ and also $G_1/G_{1tor} = \mathbb{Z}^r \cong G_2/G_{2tor} = \mathbb{Z}^{r'}$. Hence in particular $r = r'$.

4. It remains to show that $t = t'$ and $d_i = d'_i$.

To see this, it's equivalent to show the uniqueness of elementary divisors of finite abelian groups. So now we assume that G is finite abelian group. Also note that if $G_1 \cong G_2$, then $G_1(p) \cong G_2(p)$. Thus we may even assume that G is a finite abelian p-group.

Suppose now that

$$G_1 := \mathbb{Z}_{p^{a_1}} \oplus ... \oplus \mathbb{Z}_{p^{a_t}}$$
$$\cong G_2 := \mathbb{Z}_{p^{b_1}} \oplus ... \oplus \mathbb{Z}_{p^{b_s}},$$

with $a_1 \leq a_2 \leq ... \leq a_t, b_1 \leq b_2 \leq ... \leq b_s$.

Then we have $pG_1 \cong pG_2$ and $G_1/pG_1 \cong G_2/pG_2$. Note that $G_1/pG_1 \cong \mathbb{Z}_p^{c_1}$, with $c_1 = \{i | a_i > 1\}$. It follows that $c_1(G_1) = c_1(G_2)$. Similarly, we can define $c_k := \{i | a_i > k\}$ and $c_k(G_1) = c_k(G_2)$.

Moreover, $G_1[p] \cong \mathbb{Z}_p^t \cong G_2[p] \cong \mathbb{Z}_p^s$. Hence $t = s$.

Since $t, c_1(G_1), c_2(G_1)...$ determine $a_1, ..., a_t$ uniquely and $s, c_1(G_2), c_2(G_2)...$ determine $b_1, ..., b_s$ uniquely. It follows that $t = s$ and $a_i = b_i$ for all i.

2.8. **Nilpotent groups, solvable groups.** Given a group G, if G has a normal subgroup N, then we have a quotient group G/N. One can expect that knowing N and G/N would give some information on G. In this section, we are going to introduce the general technique of this idea.

Let G be a group. If G has no non-trivial normal subgroup, then G is said to be **simple**.

In general, there are two natural way to produce normal subgroups. The first one is the the center $Z(G)$. It is a normal subgroup of G. And we have the canonical projection $G \to G/Z(G)$. Let $C_2(G)$ be the inverse image of $Z(G/Z(G))$ in G. By the correspondence theorem, $Z(G/Z(G))$ is a normal subgroup of $G/Z(G)$ hence $C_2(G)$ is a normal subgroup of G. And then let $C_3(G)$ to be the inverse image of $Z(G/C_2(G))$. By doing this inductively, one has an ascending chain of normal subgroups

$$\{e\} < C_1(G) := Z(G) < C_2(G) < ...$$

Notice that by the construction, each $C_i(G) \lhd G$ and $C_{i+1}(G)/C_i(G)$ is abelian.

Definition 2.8.1. *G is nilpotent if $C_n(G) = G$ for some n.*

Proposition 2.8.2. *A finite p-group is nilpotent.*

Proof. We use the fact that a finite p-group has non-trivial center. Thus one has $C_i \lneqq C_{i+1}$. The group G has finite order thus the ascending chain must terminates, say at C_n. If $C_n \neq G$, then G/C_n has non-trivial center. One has $C_n \lneqq C_{n+1}$ which is impossible. Hence $C_n = G$. □

Theorem 2.8.3. *If H, K are nilpotent, so is $H \times K$.*

Proof. The key observation is that $Z(H \times K) = Z(H) \times Z(K)$. Then inductively, one proves that $C_i(H \times K) = C_i(H) \times C_i(K)$. If $C_n(H) = H, C_m(K) = K$ then $C_l(H \times K)$ for $l = max(m, n)$. □

Lemma 2.8.4. *Let G be a nilpotent group and $H \lneq G$ be a proper subgroup. Then $H \lneq N_G(H)$.*

Proof. Let $C_0(G) = \{e\}$. Let k be the largest index such that $C_k(G) < H$. Then $C_{k+1}(G) \nless H$. Pick $a \in C_{k+1} - H$, then for every $h \in H$, we have $C_k ha = C_k h C_k a = C_k a C_k h = C_k ah$ for $C_{k+1}/C_k = Z(G/C_k(G))$. Thus $aha^{-1} \in C_k h \subset H$ for all $h \in H$. That is $a \in N_G(H) - H$. □

Then we are ready to prove the following:

Theorem 2.8.5. *A finite group is nilpotent if and only if it's a direct product of Sylow p-subgroups.*

Proof. By the previous two results, it's clear that a direct product of Sylow p-subgroups is nilpotent.

Conversely, if G is nilpotent, then we will prove that every Sylow p-subgroup is a normal subgroup of G. By checking the decomposition criterion, one has the required decomposition.

It remains to show that if P is Sylow p-subgroup, then $P \lhd G$.
To this end, it suffices to prove that $N_G(P) = G$. By applying this Claim to $N_G(P)$, then it says that $N_G(P)$ can't be a proper subgroup of G since $N_G(N_G(P)) = N_G(P)$. Thus it follows that $N_G(P) = G$. $\square$

Example 2.8.6.

Let $G = D_{12} = \{x^i y^j | x^6 = y^2 = e, xy = yx^5\}$. One of it's Sylow 2-subgroup is $\{e, x^3, y, x^3y\}$ isomorphic to V_4 and it's Sylow 3-subgroup is $\{e, x^2, x^4\} \cong \mathbb{Z}_3$.

However $Z(G) = \{e, x^3\}$ and $G/Z(G) \cong D_6 \cong S_3$ and $Z(S_3) = \{e\}$. Thus G is not nilpotent. And therefore, $D_{12} \ncong V_4 \times \mathbb{Z}_3$. $\square$

We have seen that we have a series of subgroup by taking centers. Another natural construction is to take commutators.

Definition 2.8.7. *Let G be a group. The commutator of G, denoted G' is the subgroup generated by the subset $\{aba^{-1}b^{-1} | a, b \in G\}$.*

Roughly speaking, the subgroup G' measures the non-commutativity of a group. More precisely, $G' = \{e\}$, if and only G is abelian. The smaller G', the more commutative it is.

Proposition 2.8.8. *We have:*
1. $G' \lhd G$,
2. and G/G' is ableian.
3. if $N \lhd G$, then G/N is abelian if and only if $G' < N$.

Proof. 1.) for all $g \in G$, $g(aba^{-1}b^{-1})g^{-1} \in G'$, hence $gG'g < G'$. So $G' \lhd G$.
2.) $aG'bG' = abG' = ab(b^{-1}a^{-1}ba)G' = baG' = bG'aG'$.
3.) Consider $\pi : G \to G/N$. If G/N is abelian, then $\pi(aba^{-1}b^{-1}) = e$, hence $G' < N$. Conversely, if $G' < N$, we have a surjective homomorphism $G/G' \to G/N$. G/G' is abelian, hence so is it homomorphic image G/N. $\square$

Definition 2.8.9. *We can define the the commutator inductively, i.e. $G^{(2)} := (G')'$, etc. The $G^{(i)}$ is called the i-th derived subgroup of G. It's clear that $G > G' > G^{(2)} > \ldots$.*

A group is solvable is $G^{(n)} = \{e\}$ for some n.

Example 2.8.10.

Take $G = S_4$. The commutator is the smallest subgroup that G/G' is abelian. Since the only non-trivial normal subgroups of S_4 are V, A_4. It's clear that $G' = A_4$ (Or one can prove this by hand). Similarly, one finds that $G^{(2)} = A_4' = V$, and $G^{(3)} = \{e\}$. Hence S_4 is solvable. $\square$

Another useful description of solvable groups is the groups with *solvable series.*

Definition 2.8.11. *A groups G has a subnormal series if there is a series of subgroups of G*

$$G = H_0 > H_1 > H_2 > ... > H_n,$$

such that $H_i \lhd H_{i-1}$ for all $1 \leq i \leq n$.

A subnormal series is a solvable series if $H_n = \{e\}$ and H_{i-1}/H_i is abelian for all $1 \leq i \leq n$.

A subnormal series is a normal series if all H_i are normal subgroups of G.

Theorem 2.8.12. *A group is solvable if and only it has a solvable series.*

Proof. It's clear that $G > G' > ...G^{(n)} = \{e\}$ is a solvable series. It suffices to prove that a group with a solvable series is solvable. Suppose now that G has a sovable series $\{e\} = H_n < ... < H_0 = G$. First observe that $G' < H_1$ since G/H_1 is abelian. We claim that $G^{(i)} < H_i$ for all i inductively. Which can be proved by the observation that the intersection of the series $\{e\} = H_n < ... < H_0 = G$ with $G^{(i)}$ gives a solvable series of $G^{(i)}$. □

Example 2.8.13.

A finite p-group has a solvable series, hence is solvable.

Moreover, a nilpotent group is solvable. To see this, let G be a nilpotent group. Then there exist a series

$$\{e\} < C_1(G) := Z(G) < C_2(G) < ... < C_n(G) = G.$$

Notice that $C_{i+1}(G)/C_i(G) = Z(G/C_i(G))$ is abelian. Therefore this is a solvable series. □