1 Further Topics in Group Theory

1.1 p-Groups, Nilpotent Groups, and Solvable Groups

Definition. A *maximal subgroup* of a group G is a proper subgroup M of G such that there is no subgroups H of G with $M < H < G$.

Theorem 1. Let p be a prime and let P be a group of order p^a, $a \geq 1$. Then

1. The center of P is nontrivial: $Z(P) \neq 1$.
2. If H is a nontrivial normal subgroup of P then H contains a subgroup of order p^b that is normal in P for each divisor p^b of $|H|$. In particular, P has a normal subgroup of order p^b for every $b \in \{0, 1, \ldots, a\}$.'
3. If $H < P$ then $H < N_P(H)$ (i.e., every proper subgroup of P is a proper subgroup of its normalizer in P).
4. Every maximal subgroup of P is of index p and is normal in P.

Definition.

1. For any (finite or infinite) group G define the following subgroups inductively:

   $$Z_0(G) = 1 \qquad Z_1(G) = Z(G)$$

   and $Z_{i+1}(G)$ is the subgroup of G containing $Z_i(G)$ such that

   $$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$$

   (i.e., $Z_{i+1}(G)$ is the complete preimage in G of the center of $G/Z_i(G)$ under the natural projection). The chain of subgroups

   $$Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \ldots$$

   is called the *upper central series of* G. (The use of the term "upper" indicates that $Z_i(G) \leq Z_{i+1}(G)$.)
2. A group G is called *nilpotent* if $Z_c(G) = G$ for some $c \in \mathbb{Z}$. The smallest c is called the *nilpotence class* of G.

Note.

1. If G is abelian then it is nilpotent since $G = Z(G) = Z_1(G)$.
2. The following containments are proper

   cyclic groups $\subset$ abelian groups $\subset$ nilpotent groups $\subset$ solvable groups $\subset$ all groups

3. For any finite group there must, by order considerations, be an integer n such that

   $$Z_n(G) = Z_{n+1} = Z_{n+2} = \cdots .$$

4. For infinite groups G it may happen that all $Z_i(G)$ are proper subgroups of G (so G is not nilpotent) but
$$G = \bigcup_{i=0}^{\infty} Z_i(G).$$

Proposition 2. Let p be a prime and let P be a group of order p^a. Then P is nilpotent of nilpotence class at most $a-1$ for all $a \geq 2$ (and class equal to a when $a = 0$ or 1).

Theorem 3. Let G be a finite group, let $p_1, p_2, \ldots, p_s$ be the distinct primes dividing its order and let $P_i \in Syl_{p_i}(G), 1 \leq i \leq s$. Then the following are equivalent:

1. G is nilpotent
2. if $H < G$ then $H < N_G(H)$, i.e., every proper subgroup of G is a proper subgroup of its normalizer in G
3. $P_i \trianglelefteq G$ for $1 \leq i \leq s$, i.e., every Sylow subgroup is normal in G
4. $G \cong P_1 \times P_2 \times \cdots \times P_s$.

Corollary 4. A finite abelian group is the direct product of its Sylow subgroups.

Proposition 5. If G is a finite group such that for all positive integers n dividing its order, G contains at most n elements x satisfying $x^n = 1$, then G is cyclic.

Proposition 6. (Frattini's Argument) Let G be a finite group, let H be a normal subgroup of G and let P be a Sylow p-subgroup of H. Then $G = HN_G(P)$ and $|G : H|$ divides $|N_G(P)|$.

Proposition 7. A finite group is nilpotent if and only if every maximal subgroup is normal.

Definition. For any (finite or infinite) group G define the following subgroups inductively:
$$G^0 = G, \qquad G^1 = [G, G] \quad \text{and} \quad G^{i+1} = [G, G^i].$$
The chain of groups
$$G^0 \geq G^1 \geq G^2 \geq \ldots$$
is called the *lower central series of* G. (The term "lower" indicates that $G^i \geq G^{i+1}$.)

Theorem 8. A group G is nilpotent if and only if $G^n = 1$ for some $n \geq 0$. More precisely, G is nilpotent of class c if and only if c is the smallest nonnegative integer such that $G^c = 1$. If G is nilpotent of class c then
$$G^{c-i} \leq Z_i(G) \quad \text{for all } i \in \{0, 1, 2, \ldots, c\}.$$

Note.

1. If G is abelian, we have $G' = G^1 = 1$
2. If G is a finite group there must, by order considerations, be an integer n such that
$$G^n = G^{n+1} = G^{n+2} = \cdots .$$

Definition. For any group G define the following sequence of subgroups inductively:

$$G^{(0)} = G, \qquad G^{(1)} = [G, G], \quad \text{and} \quad G^{(i+1)} = [G^{(i)}, G^{(i)}] \quad \text{for all } i \geq 1.$$

This series of subgroups is called the *derived* or *commutator series* of G.

Theorem 9. A group G is solvable if and only if $G^{(n)} = 1$ for some $n \geq 0$.

Proposition 10. Let G and K be groups, let H be a subgroup of G and let $\varphi\colon G \to K$ be a surjective homomorphism.

1. $H^{(i)} \leq G^{(i)}$ for all $i \geq 0$. In particular, if G is solvable, then so is H, i.e., subgroups of solvable groups are solvable (and the solvable length of H is less than or equal to the solvable length of G).
2. $\varphi(G^{(i)}) = K^{(i)}$. In particular, homomorphic images and quotient groups of solvable groups are solvable (of solvable length less than or equal to that of the domain group).
3. If N is normal in G and both N and G/N are solvable then so is G.

Theorem 11. Let G be a finite group.

1. (Burnside) If $|G| = p^a q^b$ for some primes p and g, then G is solvable.
2. (Philip Hall) If for every prime p dividing $|G|$ we factor the order of G as $|G| = p^a m$ where $(p, m) = 1$, and G has a subgroup of order m, then G is solvable (i.e., if for all primes p, G has a subgroup whose index equals the order of a Sylow p-subgroup, then G is solvable — such subgroups are called Sylow p-complements).
3. (Feit-Thompson) If $|G|$ is odd then G is solvable.
4. (Thompson) If for every pair of elements $x, y \in G$, $\langle x, y\rangle$ is a solvable group, then G is solvable.

1.2 Applications in Groups of Medium Order

Proposition 12.

1. If G has no subgroup of index 2 and $G \leq S_k$, then $G \leq A_k$.
2. If $P \in Syl_p(S_k)$ for some odd prime p, then $P \in Syl_p(A_k)$ and $|N_{A_k}(P)| = \frac{1}{2}|N_{S_k}(P)|$.

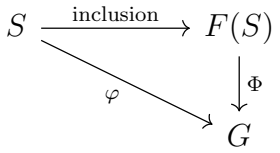
Lemma 13. In a finite group G is $n_p \not\equiv 1 \pmod{p^2}$, then there are distinct Sylow p-subgroups P and R of G such that $P \cap R$ is of index p in both P and R (hence is normal in each).

1.3 A word on Free Groups

Note. The way that a free group is defined is a bit involved and can be read on page 216

Theorem 16. $F(S)$ is a group under the binary operation defined on page 216.

Theorem 17. Let G be a group, S a set and $\varphi\colon S \to G$ a set map. Then there is a unique group homomorphism $\Phi\colon F(S) \to G$ such that the following diagram commutes:



Corollary 18. $F(S)$ is unique up to a unique isomorphism which is the identity map on the set S.

Definition. The group $F(S)$ is called the *free group* on the set S. A group F is a *free group* if there is some set S such that $F = F(S)$ — in this case we call S a set of *free generators* (or a *free basis*) of F. The cardinality of S is called the *rank* of the free group.

Theorem 19. (Schreier) Subgroups of a free group are free.

Definition. Let S be a subset of a group G such that $G = \langle S \rangle$.

1. A *presentation* for G is a pair (S, R), where R is a set of words in $F(S)$ such that the normal closure of $\langle R \rangle$ in $F(S)$ (the smallest normal subgroup containing $\langle R \rangle$) equals the kernel of the homomorphism $\pi\colon F(S) \to G$ (where π extends the identity map from S to S). The elements of S are called *generators* and those of R are called *relations* of G.

2. We say that G is *finitely generated* if there is a presentation (S, R) such that S is a finite set and we say G is *finitely presented* if there is a presentation (S, R) with both S and R finite sets.