1. Group Actions

(1.1) A **group action** of a group $G$ acting on a set $S$ is a map from $G \times S$ to $S$ (written as $g \cdot s$ or $g(s)$ for $g \in G$ and $s \in S$) such that $g_1 \cdot (g_2 \cdot s) = g_1 g_2 \cdot s$ and $e_G \cdot s = s$.

If a group $G$ is acting on a set $S$, we call $S$ a $G$-set. Suppose $S$ is a $G$-set. Define a relation $s_1 \sim s_2 \iff s_1 = g(s_2)$ for some $g \in G$, then $\sim$ is an equivalence relation. (The equivalence classes are called **orbits** of $S$ under $G$. If an orbit contains $s \in S$, then the orbit is called the **orbit of** $s$. The orbit of $s := s_G = \{g(s) | g \in G\}$.)

**Proof:** Check definition of equivalence relation.

(1.1a) Let $H \leq G$ and $S$ be the left cosets of $H$. Then $g \cdot aH = (ga)H$ is an action of $G$ on $S$, called the left multiplication action.

(1.1b) Let $H$ be a subgroup of $G$, and $a, b \in G$. Define $a \sim b \iff$ for some $g \in H$, $a = hbf^{-1}$. Verify that $\sim$ is an equivalence relation. Then $h \cdot a = hah^{-1}$ is an action of $H$ on $G$, (called the action of $H$ on $G$ by conjugation). The orbits of $G$ acting on $G$ by conjugation are called **conjugacy classes**.

(1.1c) Let $G \leq \mathcal{S}_\Omega$. Then $G$ acts on $\Omega$ by $g \cdot s = g(s)$. If $G = \langle g \rangle$, then the cycle decomposition of $g$ gives the orbits of this action.

(1.2) Suppose that $G$ is acting on a set $\Omega$. For $s \in \Omega$, the **stabilizer** of $s$ in $G$ is

$$G_s = \{g \in G | gs = s\}.$$  

The **kernel** of the action is

$$ker(G/\Omega) = \{g \in G | gs = s, \forall s \in \Omega\}.$$  

Then

(i) $G_s \leq G$. 


(ii) There is a group homomorphism $\phi : G \mapsto S_\Omega$ such that $\ker(G/\Omega) = \ker(\phi) \leq G$.

**Proof:** (i) For $g_1, g_2 \in G_s$, $g_1g_2(s) = g_1(g_2(s)) = g_1(s) = s$, and $g_1^{-1}(s) = g_1^{-1}(g_1(s)) = e(s) = s$.

(ii) $\forall g \in G$, let $\phi(g) : \Omega \mapsto \Omega$ be given by $\phi(g)(s) = g(s)$. Since $g^{-1}(g(s)) = e(s) = s$, $\phi(g)$ is onto. Since $g(s_1) = g(s_2)$ implies that $s_1 = g^{-1}(g(s_1)) = g^{-1}(g(s_2)) = s_2$, $\phi(g)$ is 1-1. Therefore, $\phi(g) \in S_\Omega$. That $g_1(g_2(s)) = (g_1g_2)(s)$ implies that $\phi$ is a group homomorphism. Finally,

$$\ker(\phi) = \{g \in G : \phi(g) = \text{ identity in } S_\Omega \} = \{g \in G : \phi(g)(s) = s, \forall s \in \Omega \} = \ker(G/\Omega).$$

(1.2a) Let $A \subseteq G$ and let $G$ acts on $S = G$ by **conjugation**, i.e. $g(x) = gxg^{-1}, \forall x \in S, g \in G$. Then $\ker(G/A) = C_G(A)$. In particular, $\ker(G/G) = Z(G)$.

**Proof** Checking definition.

(1.2b) Conjugation in $S_n$: If $\sigma = (a_1a_2 \cdots a_{k_1})(b_1b_2 \cdots b_{k_2}) \cdots$ and $\tau \in S_n$, then

$$\tau\sigma\tau^{-1} = (\tau(a_1)\tau(a_2) \cdots \tau(a_{k_1}))(\tau(b_1)\tau(b_2) \cdots \tau(b_{k_2})) \cdots$$

(1.2c) Definition: for a positive integer $n$, a partition of $n$ is a nondecreasing sequence of integers $0 < n_1 \leq n_2 \cdots n_r$ such that $\sum_{i=1}^r n_i = n$. If a permutation $\sigma \in S_n$ is the product of disjoint cycles of length $n_1, n_2, \ldots, n_r$, respectively, where $0 < n_1 < \cdots < n_r$ is a partition of $n$, then the **cycle type** of $\sigma$ is $n_1, n_2, \ldots, n_r$.

Two elements of $S_n$ are conjugate if and only if they have the same cycle type. The number of conjugacy classes of $S_n$ is the same as the number of partitions of $n$.

(1.3) A group $G$ acts **transitively** on a set $S$ if for any pair $s, s' \in S$, there if a $g \in G$ such that $g(s) = s'$. (In other words, $G$ has only one orbit: $G = s_G$ for any $s \in S$).

Let $H \leq G$, and let $G$ acts on the set $X$ of left cosets of $H$ by left multiplication $(g(H)) = (g)H$. Then

(i) $G$ acts transitively.

(ii) $G_H = H$.

(iii) $\ker(G/X) = \cap_{g \in G} gHg^{-1}$, which is the largest normal subgroup of $G$ contained in $H$.

**Proof** (i) and (ii) follows by definition.

$$\ker(G/X) = \{ g \in G | g(xH) = xH, \forall x \in G \} = \{ g \in G | x^{-1}gx \in H, \forall x \in G \} = \{ g \in G | g \in xHx^{-1}, \forall x \in G \}.$$
Thus $\ker(G/X) \leq G$. When $x = 1$, we have $\ker(G/X) \leq H$. Use definition to show that if $N \leq G$ and $N \leq H$, then $N \leq \ker(G/X)$.

**Proof** Let $G$ acts on $G$ by left (or right) multiplication.

**(1.3a)** (Cayley, Thm 4.6) Every group is isomorphic to a subgroup of a symmetric group $S_{|G|}$.

**(1.3b)** If $|G| = n < \infty$ and if $p$ is the smallest prime dividing $n$, then any subgroup $H$ of index $p$ is normal.

**Proof:** Assume $|G : H| = p$. Let $\mathcal{L}$ be the collection of left coset of $H$ in $G$ and let $G$ act on $\mathcal{L}$ by left multiplication: $g(xH) = (gx)H$. Let $K = \ker(G/\mathcal{L})$ be the kernel of the action. (want to show $H = K$!) By (1.3)(iii), $K \leq H$, and so by the index formula:


By the 1st Iso Thm, $G/K$ is iso to a subgroup of $S_p$ (since $|\mathcal{L}| = |G : H| = p$), and so by Lagrange’s Thm,

$$p|H : K| = |G/K|$$

is a factor of $|S_p| = p! \implies |H : K|$ is a factor of $(p - 1)!$.

Since $p$ is the smallest prime factor of $|G|$, $|H : K| = 1$.

**(1.4)** (Thm 4.3) If $X$ is an $G$-set and if $x \in X$, then $|x_G| = |G : G_x|$.

**Proof** Define $\phi : x_G \to \{\text{left cosets of } G_x\}$ by: $\phi(g(x)) = gG_x$. Verify that $\phi$ is well defined: If $h(x) = g(x)$, then $g^{-1}h \in G_x$ and so $gG_x = hG_x$.

$\phi$ is an injection: $\phi(g(x)) = \phi(h(x)) \iff gG_x = hG_x \iff g = hk$ for some $k \in G_x$. Hence $g(x) = hk(x) = h(x)$.

$\phi$ is onto: Definition.

**(1.5)** (Burnside) Let $G$ be a finite group and $X$ be a finite $G$-set. For each $g \in G$, define $X_g = \{x \in X | g(x) = x\}$. If $r$ denotes the number of orbits in $X$ under $G$, then

$$r|G| = \sum_{g \in G} |X_g|.$$

**Proof:** Let $(x_1)_G, (x_2)_G, \cdots, (x_r)_G$ be the orbits of $X$ under $G$. Let $P$ denote all the pairs $(x, g)$ where $g(x) = x$. $(P$ is number of 1’s in the $|X| \times |G|$ (0,1)-matrix where the $(x, g)$ entry is 1 iff $(g(x) = x$. Thus $|X_g| = \text{number of 1’s in the } g\text{th column and } |G_x| = \text{number of 1’s in the } x\text{th row.}$) Hence

$$|P| = \sum_{g \in G} |X_g| = \sum_{x \in X} |G_x|.$$
By (1.4), \(|G_x| = |G|/|x_G|\), and so
\[
\sum_{x \in X} |G_x| = |G| \sum_{x \in X} \frac{1}{|x_G|} = |G| \sum_{i=1}^{r} \sum_{x \in (x_i)_G} \frac{1}{|x_G|} = |G| \sum_{i=1}^{r} 1 = |G|r.
\]

(1.6) Let \(X\) be a \(G\)-set. The fixed points of the action is
\[
X_G = \{x \in X | g(x) = x \forall g \in G \}.
\]

\(X_G\) is the union of all single element orbits. If \((x_1)_G, (x_2)_G, \cdots, (x_s)_G\) are the orbits of \(X\) under \(G\) that are non-single-element orbits, then
\[
|X| = |X_G| + \sum_{i=1}^{s} |(x_i)_G|.
\]

**Proof** By (1.1).

(1.6a) *(The Class Equation, Cor 4.5)* Let \(|G| < \infty\) and let \(g_1, g_2, \cdots, g_r\) be representatives of the distinct conjugacy classes of \(G - Z(G)\). Then
\[
|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|.
\]

**Proof:** Let \(G\) acts on \(X = G\) by conjugation. Then \(X_G = Z(G)\) and \(C_G(g_i) = G_{g_i}\). (1.6a) follows by (1.4).

(1.6b) Let \(G\) be a group of order \(p^n\) for some prime \(p\), and let \(X\) be a finite \(G\)-set. Then \(|X| \equiv |X_G| \pmod p\).

**Proof:** By (1.4), each \(|(x_i)_G|\) is a factor of \(|G| = p^n\). (1.6b) follows then by (1.6).

(1.6c) Consider the examples when \(G = Q_8\) and when \(G = D_8\).

(1.7) Let \(G\) be a group with \(|G| = p^n\) (\(p\) a prime) and let \(X\) be a \(G\)-set. Then \(|X| \equiv |X_G| \pmod p\).

**Proof:** By (1.6) and (1.4).

(1.7a) If \(|G| = p^n\) for some prime \(p\), then \(|Z(G)| > 0\).

**Proof:** \(G\) acts on \(X = G\) by conjugation. By (1.7), \(p\) divides \(|X_G|\) and \(1 \in X_G\).

(1.7b) If \(|G| = p^2\), then \(G \in \{Z_p^2, Z_p \times Z_p\}\).

**Proof** \(G/Z(G)\) is cyclic. By (1.4.9a), \(G\) is abelian. If \(G\) has an element or order \(p^2\), then \(G = Z_p^2\). Otherwise choose \(x \in G\) with \(|x| = p\) and \(y \in G - \langle x \rangle\). Show \(G = \langle x, y \rangle \cong \langle x \rangle \times \langle y \rangle\).
(1.8) (Cauthy, Thm 5.2) If $|G| < \infty$ and if $p$ is a prime dividing $|G|$, then there is some $g \in G$ such that $|g| = p$.

**Proof** Let $X = \{(g_p, \ldots, g_2, g_1) | g_i \in G$ and $g_p \cdots g_2 g_1 = 1\}$.  
(Step 1) $|X| = |G|^{p-1} (g_p = (g_{p-1} \cdots g_2 g_1)^{-1})$. Since $p$ divides $|G|$, $p$ divides $|X|$.

(Step 2) Let $\sigma = (1, 2, \ldots, p)$ and $H = \langle \sigma \rangle$. Let $\sigma$ act on $X$ by $\sigma(g_p, \ldots, g_2, g_1) = (g_{\sigma(p)}, \ldots, g_{\sigma(2)}, g_{\sigma(1)}) = (g_1, g_p, \ldots, g_3, g_2) \in X$. By (1.7), $|X| \equiv |X_H|$ (mod $p$). By (Step 1) and since $(1, 1, 1, \ldots, 1) \in X_H$, $X_H$ has at least $p$ elements. Note that $\sigma(g_p, \ldots, g_2, g_1) = (g_p, \ldots, g_2, g_1)$ implies $a = g_1 = g_2 = \cdots = g_p$ and so $|a| = p$. 

5
Groups in this section are all finite groups.

(2.1) **Definition:** Let $G$ be a group and $p$ be a prime. A (sub)group $H$ with $|H| = p^a$ is called a $p$-**(sub)group**. A maximal $p$-subgroup of $G$ is a **Sylow $p$-subgroup** of $G$. The set of all Sylow $p$-subgroups of $G$ is $\text{Syl}_p(G)$, and $n_p = |\text{Syl}_p(G)|$.

(2.2) (Lemma 5.5) Let $H$ be a $p$-group of $G$. Then

$$[N_G(H) : H] = [G : H](\text{mod } p).$$

**Proof:** Let $L$ be the left cosets of $H$ in $G$, and let $H$ act on $L$ by $h(xH) = (hx)H$. Then $L$ is an $H$-set. Note that $|L| = [G : H]$, and note that $\forall h \in H, x \in G,$

$$hxH = xH \iff x^{-1}hx \in H \iff x \in N_G(H).$$

Hence the number of fixed points of this action is $|L_H| = [N_G(H) : H]$. Since $|H| = p^a$, by (1.6b), $|N_G(H) : H| = |L_H| = [G : H](\text{mod } p)$.

(2.2a) (Cor 5.6) Let $H$ be a $p$-subgroup of a finite group $G$. If $p$ divides $[G : H]$, then $N_G(H) \neq H$.

(2.3) **The First Sylow Theorem** (Thm 5.7) Let $G$ be a group of order $p^am$, where $a > 0$ and where $p$ is a prime not dividing $m$. Then

(i) $G$ contains a subgroup of order $p^i$ for each $i$ where $0 \leq i \leq a$,

(ii) every subgroup $H$ of $G$ of order $p^i$ is a normal subgroup of a subgroup of order $p^{i+1}$ for $1 \leq i < a$.

**Proof:** (i) By induction on $a$. Clearly $G$ has a subgroup of order 1. Suppose that $H$ is a subgroup of order $p^i$ for some $0 \leq i < a$. Since $i < a$, $p$ divides $p^{a-1}m = |G : H|$.

By (2.2a), $|N_G(H) : H| > 0$. Since $H \trianglelefteq N_G(H)$, the group $N_G(H)/H$ has $p$ as a factor, and so by Cauchy’s Theorem (1.8), $N_G(H)/H$ has a subgroup $K'$ of order $p$. Let $K = \{k \in N_G(H) | kH \in K'\}$. Then $K$ is the inverse image of a homomorphism, and so $K \leq N(G) \leq G$. Since $|K : H| = |K'| = p$, $|K| = p^{i+1}$.

(ii) Note that in (i), $H \leq K \leq N_G(H)$. Since $H \trianglelefteq N_G(H)$, $H \trianglelefteq K$.

(2.4) **The Second Sylow Theorem** (Thm 5.9) Let $G$ be a finite group and let $P_1, P_2 \in$
such that $Q$ is a prime not dividing $m$ there exists a $p$ such that $P_1 = gP_2g^{-1}$.

**Proof:** (The trick here is to let one ($P_2$, say) act on the left cosets of the other ($P_1$).) Let $\mathcal{L}$ be the collection of left cosets of $P_1$, and let $P_2$ act on $\mathcal{L}$ by

$$\forall y \in P_2, y(gP_1) = (yg)P_1.$$  

The fixed points: By (1.6b), $|\mathcal{L}P_2| \equiv |\mathcal{L}| \pmod{p}$. Since $P_1 \in Syl(G)$, $|\mathcal{L}| = |G : P_1|$ is not divisible by $p$. Hence $|\mathcal{L}P_2| > 0$. Let $zP_1 \in \mathcal{L}P_2$. Then

$$\forall y \in P_2, y(zP_1) = zP_1 \implies z^{-1}P_2z \leq P_1 \implies z^{-1}P_2z = P_1,$$

where the last equality follows by counting. Finally, set $g = z^{-1}$.

**The Third Sylow Theorem** (Thm 5.10) If $|G| = p^a m < \infty$ (where $p$ is a prime) and if $n_p = |Syl_p(G)|$, then both $n_p \equiv 1 \pmod{p}$ and $n_p | p^a m$.

**Proof: Action 1:** Fix $Q \in Syl_p(G)$. Let $Q$ act on $Syl_p(G)$ by conjugation:

$$\forall x \in Q \text{ and } \forall P \in Syl_p(G), x(P) = xPx^{-1}.$$  

The fixed points: By (1.6b), $|(Syl_p(G))_Q| \equiv |Syl_p(G)| \pmod{p}$.

$$(Syl_p(G))_Q = \{ P \in Syl_p(G) \mid xP = P \forall x \in Q \} = \{ P \in Syl_p(G) \mid Q \subseteq N_G(P) \},$$

and so $P, Q \in Syl_p(N(P))$. Apply 2nd Sylow Theorem to $N_G(P)$, there is a $g \in N_G(P)$ such that $Q = gPg^{-1} = P$, (the last equality follows from $g \in N_G(P)$). Thus $(Syl_p(G))_Q = \{ Q \}$.

By (1.6b), $n_p = |Syl_p(G)| \equiv |(Syl_p(G))_Q| = 1 \pmod{p}$.

**Action 2:** Let $G$ act on $Syl_p(G)$ by conjugation. By (2.4), the action is transitive, and so $G_P = Syl_p(G)$ is the only orbit. By (1.4), $n_p = |Syl_p(G)| = |G : G_P|$ and so by Lagrange’s theorem, $n_p$ divides $|G|$.

**Sylow’s Theorem** (A combined statement) Let $G$ be a group of order $p^a m$, where $p$ is a prime not dividing $m$.

(i) $Syl_p(G) \neq \emptyset$, and if $H$ is a $p$-subgroup of $G$ such that $[G : H] \equiv 0 \pmod{p}$, then there exists a $p$ subgroup $H'$ of $G$ such that $[H' : H] = p$.

(ii) If $P$ is a Sylow $p$-subgroup of $G$ and $Q$ is a $p$-subgroup of $G$, then there exists $g \in G$ such that $Q \leq gPg^{-1}$. In particular, any two Sylow $p$-subgroups of $G$ are conjugate in $G$.

(iii) The number of Sylow $p$-subgroups $n_p \equiv 1 \pmod{p}$ and $n_p | m$. 

7
3. Theorems on Sylow $p$-groups

In this section, we make the following assumptions: $|G| = p^a m$ for some prime $p$, where integers $a > 0$ and $m$ satisfies $(m, p) = 1$.

(3.1) Suppose that $P \in Syl_p(G)$, and $N \leq G$ such that $N_G(P) \leq N$. Then $N_G(N) = N$.

**Proof:** It suffices to show that $N_G(N) \subseteq N$. Since $N_G(N)$, $Q = xPx^{-1} \in Syl_p(G)$. Since $x \in N_G(N)$ and $P \leq N$, then $Q = xPx^{-1} \trianglelefteq xNx^{-1} = N$, and so $P, Q \in Syl_p(N)$. By 2nd Sylow Theorem, $\exists y \in N$, such that $P = yQy^{-1} = (yx)P(yx)^{-1}$. It follows that $yx \in N_G(P) \subseteq N$. But $y \in N$, and so $x \in N$.

(3.2) Suppose that $H = H_1 \cap H_2$ is maximal in the set of $\{H_i \cap H_j : H_i, H_j$ are distinct members in $Syl_p(G)\}$. Let $N = N_G(H)$. Then

(i) If $K \in Syl_p(N)$, then there exists exactly one $P \in Syl_p(G)$ such that $K = P \cap N$.
(ii) If $P \in Syl_p(G)$ such that $H \leq P$, then $P \cap N \in Syl_p(N)$.
(iii) If $K_1, K_2 \in Syl_p(N)$ are two distinct members, then $K_1 \cap K_2 = H$.
(iv) If $K \in Syl_p(N)$, then $N_K(K) = N \cap N_G(P)$ for some $P \in Syl_p(G)$ such that $H \leq P$.
(v) $[N : H] > 1$, and every Sylow $p$-subgroup of $N$ contains $H$ properly.
(vi) $|Syl_p(N)| > 1$.

**Proof:** Since $H \neq H_1$, then $N \neq N_{H_1}(H) \subseteq H_1 \cap N$. Therefore, there exists a $K \in Syl_p(N)$ such that $H \neq H_1 \cap N \leq K$. By 1st Sylow Theorem, there exists a $P \in Syl_p(G)$ such that $K \leq P$. Since

$N \neq H_1 \cap N \leq P \cap H_1,$

We must have $H_1 = P$, and so $K = P \cap N = H_1 \cap N$ (this proves (i) and (ii)).

Let $K_1, K_2 \in Syl_p(N)$ be two distinct members, and let $K \in Syl_p(N)$ be a member such that $H \leq K$. By 2nd Sylow Theorem, there exists $z \in N$ such that $K_1 = zKz^{-1}$. Since $z \in N = N_G(H)$ and since $H \leq K$, $H = zHz^{-1} \leq zKz^{-1} = K_1$. Similarly, $H \leq K_2$. Therefore, $H \subseteq K_1 \cap K_2$. By (iv) (just shown above), there exist $P_1, P_2 \in Syl_p(G)$ such that $K_1 = P_1 \cap N$. Therefore, $H \subseteq P_1 \cap P_2$. By the maximality of $H$, $H = P_1 \cap P_2 = K_1 \cap K_2$. This proves (iii).

Let $K = H_1 \cap N$. Then by checking the definition for normalizer, we have $K \triangleleft N_G(H_1) \cap$
$N$. If for any $x \in N$, $xKx^{-1} = K$, then $K \subseteq xH_1x^{-1}, \forall x \in N$, and so by (iv), $H_1 = xH_1x^{-1}$.

It follows that $x \in N_G(H_1) \cap N = K$. This would imply that

$$H_1 \cap N = K = N_G(H_1) \cap N = N_N(K).$$

This proves (iv) with $P = H_1$.

Note that $H_1 \in Syl_p(G)$ and that $H \subseteq H_1$ but $H \neq H_1$. Thus $[N : H] \equiv [G : H] \equiv 0 \mod p$ (See (2.2) in the preceding section), and so $[N : H] > 1$. This proves the first half of (v).

Recall that $H = H_1 \cap H_2$. Let $K_1 = H_1 \cap N$ and $K_2 = H_2 \cap N$. By (ii), $K_1, K_2 \in Syl_p(N)$. By (i), $K_1 \neq K_2$. Therefore, $|Syl_p(N)| > 1$. This proves (vi).

Let $K \in Syl_p(N)$. By (vi), we can find another $K' \in Syl_p(N) - \{K\}$. By (iii), $H = K \cap K'$. This proves the later half of (v).
4. Nilpotent and Solvable Groups

(4.1) **(The Central Series)** Let $G$ be a group, and let $C(G)$ denote the center of $G$; and define

\[ C_0(G) = \{e\} \]
\[ C_1(G) = C(G) \]
\[ C_2(G) = \text{inverse image of } C(G/C_1(G)) \text{ under the projection } G \hookrightarrow G/C_1(G) \]
\[ \cdots = \cdots \]
\[ C_i(G) = \text{inverse image of } C(G/C_{i-1}(G)) \text{ under the projection } G \hookrightarrow G/C_{i-1}(G) \]
\[ \cdots = \cdots \]

Then, each $C_i(G) \subseteq G$, and the series

\[ \{e\} < C_1(G) < C_2(G) \cdots \]

is called **the ascending central series** of $G$. A group $G$ is nilpotent if for some integer $n$, $G_n = G$.

(4.1a) If $G_n = G$, then $G_{n+1} = G$; and for each $i$, $C(G/C_i(G)) = C_{i+1}(G)/C_i(G)$.

(4.1b) Any abelian group is nilpotent.

(4.1c) (Thm 7.2) Every finite $p$-group is nilpotent. (By the class equation).

(4.1d) (Thm 7.3) The direct product of a finite number of nilpotent groups is nilpotent.

**Proof:** It suffices to show the case when the factor number is 2.

(i) If $H_1 \leq H$ and $K_1 \leq K$, then $H/H_1 \times K/K_1 \cong (H \times K)/(H_1 \times K_1)$.

(ii) $C_i(H) \times C_i(K) = C_i(H \times K)$

As (i) is a special case of (1.8) in Products of Groups, we only need to prove (ii). Note first that

\[ C_1(H \times K) = C(H \times K) = C(H) \times C(K) = C_1(H) \times C_1(K). \]

In particular, for any $i$,

\[ C(H/C_i(H) \times K/C_i(K)) = [C(H/C_i(H)) \times C(K/C_i(K))]. \]
Fixed an \( i \geq 1 \). Assume inductively that

\[ C_i(H \times K) = C_i(H) \times C_i(K). \]

Then \( C_i(H) \triangleleft H \) and \( C_i(K) \triangleleft K \). Let \( \pi_H : H \mapsto H/C_i(H) \) and \( \pi_K : K \mapsto K/C_i(K) \) be the canonical projections, and \( \pi = (\pi_H, \pi_K) : H/C_i(H) \times K/C_i(K) \mapsto (H \times K)/C_i(H \times K) \) be the homomorphism defined componentwise. By (i), there is an isomorphism

\[
\psi : H/C_i(H) \times K/C_i(K) \mapsto (H \times K)/(C_i(H) \times C_i(K)) = (H \times K)/C_i(H \times K).
\]

Let \( \phi = \psi \cdot \pi : H \times K \mapsto (H \times K)/C_i(H \times K) \). Then

\[
C_{i+1}(H \times K) = \phi^{-1}[C((H \times K)/C_i(H \times K))] = \pi^{-1}\psi^{-1}[C((H \times K)/C_i(H \times K))]
\]

\[
= \pi^{-1}[C(H/C_i(H)) \times K/C_i(K)]
\]

\[
= \pi^{-1}[C(H/C_i(H))] \times \pi_K^{-1}[C(K/C_i(K))]
\]

\[
= C_{i+1}(H) \times C_{i+1}(K).
\]

Thus by induction, (ii) always holds.

Suppose that both \( H \) and \( K \) are nilpotent. Then

\[
\{e_H\} < C_1(H) < C_2(H) < \cdots < C_m(H) = H,
\]

and

\[
\{e_K\} < C_1(K) < C_2(K) < \cdots < C_n(K) = K.
\]

We may assume that \( m \geq n \). Then \( C_{n+1}(K) = \cdots C_m(K) = K \) and so,

\[
\{e_H\} \times \{e_K\} < C_1(H) \times C_1(K) < \cdots < C_m(H) \times C_m(K).
\]

By (ii), (only the last equality is needed),

\[
\{e_{H \times K}\} < C_1(H \times K) < \cdots < C_m(H \times K) = H \times K.
\]

(4.2) (Lemma 7.4) Let \( G \) be nilpotent, and let \( H < G \) be proper. Then \( H < N_G(H) \) is also proper.
Proof: \( G \) is nilpotent \( \implies G_m = G \). Let \( n \) be the largest such that \( G_n < H \). Since \( H \neq G, n < m \). Pick \( a \in C_{n+1}(H) - H \). Then \( a \in N_G(H) - H \).

(4.3) If \( |G| < \infty \), and if \( P \in Syl_p(P) \), then \( N_G(N_G(P)) = N_G(P) \).

Proof: This is a special case of (3.1). A direct proof is as follows. \( P \leq N_G(P) \). Since \( \forall x \in N_G(N_G(P)) \implies x(N_G(P))x^{-1} = N_G(P), xPx^{-1} = P \implies x \in N_G(P) \).

(4.4) (Prop. 7.5) A finite group is nilpotent if and only if \( G \) is the direct product of its Sylow subgroups.

Proof: (Sufficiency) If \( G \) is the direct product of its Sylow subgroups, then by (4.1c) and (4.1d), \( G \) is nilpotent.

(Necessity) Let \( G \) be nilpotent. If \( G \) itself is a \( p \)-group, then done. Assume that \( G \) is not a \( p \)-group.

Step 1 Every Sylow \( p \)-subgroup is normal in \( G \).

Let \( P \in Syl_p(G) \). Then \( P \neq G \). By (4.2), \( P \neq N_G(P) \). If \( N_G(H) \neq G \), then by (4.2) (with \( H \) replaced by \( N_G(H) \)), \( N_G(P) \neq N_G(N_G(H)) \). On the other hand, by (4.3), \( N_G(P) = N_G(N_G(H)) \). This implies \( N_G(H) = G \) and so \( Syl_p(G) = \{P\} \).

Step 2 If \( P_i \) is a Sylow \( p_i \)-subgroup, and \( P_j \) is a Sylow \( p_j \)-subgroup, where \( p_i \) and \( p_j \) are two distinct primes, then \( P_i \cap P_j = \{e\} \) and \( P_iP_j = P_jP_i \).

Consider the order of an element in the intersection to see \( \{e\} = P_i \cap P_j \). For \( x \in P_i, y \in P_j \), \( xyx^{-1}y^{-1} \in P_iP_j \), as \( P_i \) and \( P_j \) are normal in \( G \).

Step 3 Suppose \( |G| = p_1^{n_1}p_2^{n_2} \cdots p_m^{n_m} \), where \( p_1, p_2, \ldots, p_m \) are the distinct primes dividing \( |G| \), and \( P_1, P_2, \ldots, P_m \) are the corresponding Sylow \( p_i \)-subgroups, then \( G = P_1P_2 \cdots P_m \).

By Lagrange and Step 2, every element in \( P_1 \cdots P_{i-1}P_{i+1} \cdots P_m \) has order dividing

\[
p_1^{n_1}p_2^{n_2} \cdots p_{i-1}^{n_{i-1}}p_{i+1}^{n_{i+1}} \cdots p_m^{n_m},
\]

and so

\[
P_1 \cap P_1 \cdots P_{i-1}P_{i+1} \cdots P_m = \{e\}.
\]
As $P_1 P_2 \cdots P_m \leq G$, and as 

$$p_1^{n_1} p_2^{n_2} \cdots p_m^{n_m} = |P_1 P_2 \cdots P_m| \leq |G| = p_1^{n_1} p_2^{n_2} \cdots p_m^{n_m},$$

we must have $G = P_1 P_2 \cdots P_m$.

Combine Step 1 and Step 3 to conclude that 

$$G \cong P_1 \times P_2 \times \cdots \times P_m.$$

(4.5) (Thm 7.8) Let $G$ be a group and let $a, b \in G$. The element $aba^{-1}b^{-1}$ is called a \textbf{commutator} of $G$. The subgroup 

$$G' = \langle aba^{-1}b^{-1} : a, b \in G \rangle$$

is called the \textbf{commutator subgroup} of $G$. Moreover,

(i) $G'$ is an invariant subgroup of $G$, and so $G' \trianglelefteq G$.

(ii) $G/G'$ is abelian.

(iii) Suppose $N \trianglelefteq G$. Then $G/N$ is abelian if and only if $G' \triangleleft N$.

\textbf{Proof}: (i) $\forall g \in G$, and $\forall a, b, \in G$, 

$$g(aba^{-1}b^{-1})g^{-1} = g(ab)g^{-1}(ab)^{-1}a(bg)a^{-1}(bg)^{-1}bgb^{-1}g^{-1}.$$ 

(ii) $\forall a, b \in G$, $ab = aba^{-1}b^{-1}ba$, and so $(ab)G' = (ba)G'$.

(iii) Suppose that $(ab)N = (ba)N \iff aba^{-1}b^{-1} \in N$.

(4.6) Let $G^{(0)} = G$. For each $i \geq 1$, define $G^{(i)} = (G^{(i-1)})'$. Then 

(i) $\cdots \subseteq G^{(i)} \subseteq G^{(i-1)} \cdots \subseteq G^{(1)} \subseteq G^{(0)} = G$.

(ii) $\forall i$, $G^{(i)} \trianglelefteq G$.

\textbf{Proof}: (4.5) $\implies$ (ii) holds when $i = 1$. Then argue by induction and use the correspondence in the isomorphism theorems. (Another way to see this is that each of the $G^{(i)}$ is an invariant subgroup.)

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

13
Every nilpotent group is solvable.

**Proof:** \( G \) is nilpotent \( \implies C_n(G) = G \).

\[ C(G/G_{n-1}(G)) = C_n(G)/C_{n-1}(G) \text{ is abelian} \implies G^{(1)} < C_{n-1}(G). \]

Similarly,

\[
G^{(2)} = (G^{(1)})' < C_{n-1}(G)' < C_{n-2}(G)
\]

\[
\vdots \quad \vdots
\]

\[
G^{(n)} = (G^{(1)})' < C_1(G)' = C(G) = \{e\}
\]

(4.9) (Thm 7.11)

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

(ii) Suppose \( N \leq G \). Then \( G \) is solvable if and only if both \( N \) and \( G/N \) are solvable.

**Proof:** (i). Suppose \( f : G \to H \) is an epimorphism. Then

\[
f(G^{(1)}) = \langle \{ f(a)f(b)f(a)^{-1}f(b)^{-1} : a, b \in G \} \rangle = H^{(1)},
\]

and

\[
f(G^{(i)}) = \langle \{ f(a)f(b)f(a)^{-1}f(b)^{-1} : a, b \in G^{(i-1)} \} \rangle = \langle \{ f(a)f(b)f(a)^{-1}f(b)^{-1} : a, b \in H^{(i-1)} \} \rangle = H^{(i)}.
\]

If \( H < G \), then \( G^{(i)} \cap H = H^{(i)} \).

(ii). Let \( \pi : G \to G/N \) be the canonical map. Note that \( \pi(G^{(n)}) = (G/N)^{(n)} = \{e_{G/N}\} \). It follows that \( G^{(n)} \leq \text{Ker} \pi = N \). By (i), as a subgroup of a solvable group \( N \), \( G^{(n)} \) is also solvable.

(4.10) If \( n \geq 5 \), then \( S_n \) is not solvable.

**Proof** Suppose that \( S_n \) is solvable. Then by (4.9), \( A_n \), as a subgroup of \( S_n \), must be solvable. Consider the commutator group \( A'_n \). Since \( A_n \) is not abelian, \( A'_n \neq \{e\} \). Since \( A_n \) is simple, and since \( A'_n \triangleleft A_n \), we must have \( A'_n = A_n \). It follows that \( A^{(i)}_n = A_n \) for any \( i \geq 1 \), and so \( A_n \) cannot be solvable.