Chapter II

Action of a Group on a Set and Permutation Representations

One of the most effective methods to study an abstract group is to compare it with known groups, that is, to consider homomorphisms from the given group into groups, the structure of which is already known, or in which it is much more easier to make concrete calculations. The first candidates of known groups are matrix groups, in other words, groups of invertible linear transformations of a finite dimensional vector space and permutation groups. In this chapter we shall give the basic notions necessary for dealing with cases arising from the second possible choice.

2.1. Group Actions

2.1.1. Definition. Let $G$ be a group and $X$ a nonempty set. We say that $G$ acts on $X$ on the left, if there exists a map \( \mu : G \times X \to X \) such that the following two conditions are satisfied:

A. I) \( \mu(e, x) = x \) for all \( x \in X \),

A. II) \( \mu(g_1 g_2, x) = \mu(g_1, \mu(g_2, x)) \) for all \( g_1, g_2 \in G \) and all \( x \in X \).

For the sake of simplicity we shall denote the image of \((g, x) \in G \times X\) under \( \mu \) by \( gx \), if the action \( \mu \) of \( G \) on \( X \) is clear from the context. With this notation the above conditions are expressed as

A. I) \( e \cdot x = x \) for all \( x \in X \),

A. II) \( (g_1 g_2) x = g_1(g_2 x) \) for all \( g_1, g_2 \in G \) and for all \( x \in X \).

2.1.2. Remark. In a similar way we can define an action of $G$ on $X$ on the right. Explicitly, an action of $G$ on $X$ on the right consists of a map \( \cdot : X \times G \to X \) written \( (x, g) \mapsto xg \) such that the following hold:

(i) \( xe = x \) for all \( x \in X \)

(ii) \( x(g_1 g_2) = (xg_1)g_2 \) for all \( x \in X \) and for all \( g_1, g_2 \in G \).
2.1.3. **Remark.** Assume that $G$ act on $X$ on the left. Then one may construct an action of $G$ on $X$ on the right, by defining, for all $g \in G$ and $x \in X$, $xg = g^{-1}x$. Similarly, a left action can be constructed from a right action.

Throughout this text, we consider only left actions unless otherwise stated.

2.1.4. **Examples.**

(a) For any group $G$ and any nonempty set $X$ we have the trivial action $\mu : G \times X \to X$ with $\mu(g, x) = x$ for all $g \in G$ and any $x \in X$.

(b) Let $G$ be a group and $H$ a subgroup of $G$ and $X = \{xH|x \in G\}$ the set of all left cosets of $G$. Then $G$ acts on $X$ by multiplication from left, that is, $L : G \times X \to X$ given by $L(g, xH) := g(xH) = (gx)H$ is an action of $G$ on $X$.

Let $Y = \{Hy|y \in G\}$, then $G$ acts on $Y$ by multiplication from right, if we define the action by $R : G \times Y \to Y$ given as $R(g, Hy) := (Hy)g^{-1} = H(yg^{-1})$.

Observe that $R' : G \times Y \to Y$ given by $R'(g, Hy) := (Hy)g$ does not satisfy (A. II):

$$R'(g_1g_2, Hy) = (Hy)(g_1g_2) = ((Hy)g_1)g_2 = R'(g_2, (Hy)g_1) = R'(g_2, R'(g_1, Hy))$$

is not equal to $R'(g_1, R'(g_2, Hy))$ in general.

(c) Let $G$ be a group and $N$ a normal subgroup of $G$. Then $G$ acts on $X = N$ by conjugation that is,

$$T : G \times X \to X$$

given by $T(g, x) := gxg^{-1}$ is an action of $G$ on $X$.

Throughout the text, we shall use the notation $x^g$ for $gxg^{-1}$.

(d) Let $G$ be a group and $H$ a subgroup of Aut $G$. Then $H$ acts on $G$ in a natural way: $\mu : H \times G \to G$, $\mu(\alpha, g) : = \alpha(g)$ for all $\alpha \in H$ and $g \in G$.

(e) Let $\mu : G \times X \to X$ be an action of the group $G$ on the nonempty set $X$.

i) If $P(X)$ denotes the set of all subsets of $X$, then $\mu_1 : G \times P(X) \to P(X)$ defined by $\mu_1(g, \phi) = \phi$ and $\mu_1(g, A) = \{g \cdot a|a \in A\}$, if $\phi \neq A \subseteq X$. for all $g \in G$, is an action of $G$ on $P(X)$.

ii) If $H$ is a subgroup of $G$, then $\mu_{|H \times X} : H \times X \to X$ with $\mu_{|H \times X}(h, x) = \mu(h, x)$ is an action of the group $H$ on $X$.

iii) If $\phi \neq Y \subseteq X$ and $gy \in Y$ for all $y \in Y$ and $g \in G$, then $\mu_{|G \times Y}$ gives an action of $G$ on $Y$. 

2.1.5. Definition. Let $G$ be a group, $X$ and $Y$ be nonempty sets and $\mu_1 : G \times X \to X$ and $\mu_2 : G \times Y \to Y$ be two actions of $G$ on the sets $X$ and $Y$, respectively. We say $\mu_1$ is equivalent to $\mu_2$ if there exists a bijection $\nu : X \to Y$ such that

$$\mu_2(g, \nu(x)) = \nu(\mu_1(g, x))$$

for all $g \in G$, and $x \in X$, that is, the following diagram commutes.

2.2. Orbits and Stabilizers

2.2.1. Theorem. Let $G$ be a group and assume that $G$ acts on a nonempty set $X$.

(a) The relation $\sim$ on $X$ defined by $x \sim y$ iff there exists $g \in G$ with $gx = y$, is an equivalence relation on $X$. The equivalence classes of $\sim$ on $X$ are called the orbits of $G$ on $X$. For $x \in X$, $O_x = \{gx | g \in G\}$ is the orbit that contains $x$.

(b) The set $\{g \in G | gx = x\}$, $x \in X$, of all elements of $G$ fixing $x \in X$, is a subgroup of $G$. It will be denoted by $G_x$ and called the stabilizer of $x$ in $G$.

(c) For $x \in X$, $|O_x| = |G : G_x|$. In particular, if $G$ is finite, then the length of any orbit of $G$ on $X$ divides the order of $G$.

(d) For any $x \in X$ and any $g \in G$ we have $G_x^g = gG_xg^{-1} = G_{gx}$.

Proof. (a) Follows by straightforward verification.

(b) For any $g_1, g_2 \in G_x$ we have $(g_1g_2^{-1})x = g_1(g_2^{-1}x) = g_1x = x$, since $g_2x = x$ implies $g_2^{-1}x = g_2^{-1}(g_2x) = (g_2^{-1}g_2)x = ex = x$ for any $x \in X$. Thus $G_x$ is a subgroup of $G$.

(c) Let $\phi : \{gG_x | g \in G\} \to O_x$ be given by $\phi(gG_x) = gx$. Since for any other representative $g'$ of the coset $gG_x$ we have $h \in G_x$ such that $g' = gh$ we let that $g'x = (gh)x = g(hx) = gx$, thus $\phi$ is a well defined map.
We have \( g_1x = \phi(g_1G_x) = \phi(g_2G_x) = g_2x \) if and only if \( g_1^{-1}g_2 \in G_x \), i.e. \( g_1G_x = g_2G_x \). Hence \( \phi \) is injective. Obviously \( \phi \) is surjective. Hence \( |O_x| = |G : G_x| \).

(d) For any \( h \in G_x \) we have \( (ghg^{-1})(gx) = gx \). Hence \( gG_xg^{-1} \leq G_{gx} \).

Conversely if \( y \in G_{gx} \), then \( y(gx) = gx \) and hence \( (g^{-1}yg)(x) = x \). Thus \( y = g(g^{-1}yg)g^{-1} \in gG_xg^{-1} \), since \( g^{-1}yg \in G_x \). Hence \( gG_xg^{-1} = G_{gx} \). \( \square \)

2.2.2. Definition. Let \( G \) be a group and assume that \( G \) acts on the set \( X \). We say that \( G \) acts transitively on \( X \) (or \( G \) is transitive on \( X \)) if \( X \) is an orbit of \( G \) on \( X \), that is, if for any \( x, y \in X \) there exists \( g \in G \) with \( gx = y \). (If \( |X| = n \), and \( x \in X \), then \( |G| = n|G_x| \) by (2.2.1c)). We say that \( G \) acts regularly on \( X \) (or \( G \) is regular on \( X \)) if \( gx = x \) for some \( x \in X \) implies that \( g = e \), that is \( G_x = \{e\} \) for each \( x \in X \).

2.2.3. Example. Let \( G \) be a group and \( H \) a subgroup of \( G \), \( T \) a transversal for \( H \) in \( G \) and \( X = \{tH\mid t \in T\} \). \( G \) acts on \( X \) by left multiplication. This action is transitive, since for any \( t_1, t_2 \in T \) we have \((t_1t_2)H = t_1H \). The stabilizer of \( H \in \{tH\mid t \in T\} \) is \( \{g \in G\mid gH = H\} = H \). Thus by (2.2.1c) we have \( G_{tH} = tHt^{-1} \).

2.2.4. Theorem. Let \( G \) be a group.

(a) \( G \) acts on the set \( X = G \) by conjugation, that is, \((g, x) \mapsto x^g = gxg^{-1} \). The orbits of \( G \) on the set \( G \) by this action are called conjugacy classes of \( G \). If \( x \in G \), then the stabilizer of \( x \) in \( G \) is \( G_x = \{g \in G\mid x^g = x\} = \{g \in G\mid gx = xg\} = C_G(x) \), the centralizer of \( x \) in \( G \). \( \bigcap_{x \in G} C_G(x) = Z(G) \) is called the center of \( G \) and is obviously normal in \( G \). If \( x^g = y \), then \( C_G(x) \supseteq C_G(y) \). The conjugacy class of \( G \) containing \( x \) consists of \( x \) alone if and only if \( x \in Z(G) \).

(b) Let \( G \) be a finite group and \( C_1 = \{e\}, C_2, \cdots, C_h \) be the conjugacy classes of \( G \) and let \( C_1, C_2, \cdots, C_r \) be the conjugacy classes of \( G \) consisting of a single element, \( r = |Z(G)| \), and \( x_i \in C_i, i = r + 1, \cdots, h \). Then
\[
|G| = |Z(G)| + \sum_{i=r+1}^{h} |G : C_G(x_i)| \quad (\text{class equation})
\]

(c) \( N \) is a normal subgroup of \( G \) if and only if \( N \) is a subgroup of \( G \) which is the union of some conjugacy classes of \( G \).

Proof. (a) Trivial.
(b) Since the conjugacy classes of $G$ are orbits of $G$ on the set $X = G$ we have
$$|G| = \sum_{i=1}^{h} |C_i|.$$ By the last statement of (a) we have $|G| = \sum_{i=1}^{h} |C_i| + |Z(G)|$. On the other hand $|C_i| = |G : G_{x_i}|$ by (2.2.1) and hence $|C_i| = |G : C_G(x_i)|$ by (a).

(c) Obvious.

\[ \square \]

2.3. Cauchy’s Theorem and $p$-Groups

2.3.1. Definition. A group $G$ is called a $p$-group, $p$ a prime, if $o(g) = p^k$ for some $k \in \mathbb{N}$, for any $g \in G$. For example, $C_{p^n}$ is a $p$-group.

2.3.2. Theorem. (Cauchy) If $G$ is a finite group and $p$ is a prime dividing $|G|$ then $G$ contains an element of order $p$.

Proof. (J.H. Mc Kay) Let $X = \{(g_0, g_1, g_2, \ldots, g_{p-1}) | g_i \in G, i \in \mathbb{Z}_p, g_0 g_1 \cdots g_{p-1} = e \}$. Since $g_{p-1}$ is uniquely determined by the first (arbitrary) $p - 1$ entries as $g_{p-1} = (g_0 g_1 \cdots g_{p-2})^{-1}$ we have $|X| = |G|^{p-1}$. Consider the map $\mu : \mathbb{Z}_p \times X \to X$ given by $\mu(k(g_0 g_1 \cdots g_{p-1})) = (g_k, g_{k-1}, \ldots, g_{p-1+k})$ defines an action of $\mathbb{Z}_p$ on $X$, since

(a) $g_0, g_1, \ldots, g_{k-1}g_k \cdots g_{p-1} = e$ implies that

$(g_k \cdots g_{p-1})^{-1}(g_k \cdots g_{p-1})(g_0 g_1 \cdots g_{k-1})(g_k \cdots g_{p-1}) = e$

and hence $g_k \cdots g_{p-1}g_0 g_1 \cdots g_{k-1} = e = g_k g_{k+1} \cdots g_{i+k} \cdots g_{p-1+k}$. Thus $\mu(k(g_0 g_1 \cdots g_{p-1})) \in X$.

(b) $\mu(0, x) = \mu(0, (g_0, g_1, g_2, \cdots, g_{p-1})) = (g_0, g_1, \cdots, g_{p-1}) = x$ for any $x \in X$ and

(c) $\mu(k + \ell, (g_k, g_{k+1}, \cdots, g_{p-1+\ell})) = \mu(k, \mu(\ell, (g_0, g_1, \cdots, g_{p-1+\ell})))$ for any $k, \ell \in \mathbb{Z}_p$ and any $(g_0, \cdots, g_{p-1}) \in X$.

Let $X_1, X_2, \cdots, X_s$ be the orbits of $\mathbb{Z}_p$ on $X$. Then $|X| = |G|^{p-1} = \sum_{i=1}^{s} |X_i|$ where $|X_i|$ divides $|\mathbb{Z}_p| = p$. Let $r$ be the number of orbits $X_i$ with $|X_i| = 1$. Then $|X| = r + \sum_{|X_i|=p} |X_i|$ and hence, since $p||G|$ and hence $p||X|$, $r \equiv 0 \mod p$. On the other hand $r \geq 1$, since $x_0 = (e, e, \cdots, e) \in X$ and $\mu(k, x) = x$ for all $k \in \mathbb{Z}_p$. Thus there exists $x_1 \in X$ with $x_1 \neq x_0$ and $\mu(k, x_1) = x_1$ for all $k \in \mathbb{Z}_p$.

Let $x_1 = (g_0, g_1, \cdots, g_{p-1})$. Then $(g_0, g_1, \cdots, g_{p-1}) = (g_1, g_2, \cdots, g_{p-1}, g_0) = (g_2, \cdots, g_0, g_1) = \cdots = (g_{p-1}, g_0, g_1, \cdots, g_{p-2})$ implies that $g_0 = g_1 = \cdots = g_{p-1} = \cdots = g_{p-1}$.
g \in G$ with $g \neq e$. Then $o(g) = p$, since $g_0 g_1 \cdots g_{p-1} = e$. 

**2.3.3. Corollary.** A finite group $G$ is a $p$-group if and only if $|G| = p^n$ for some $n$.

*Proof.* follows immediately from (2.3.2).

**2.3.4. Theorem.** Let $G$ be a finite $p$-group.

(a) If $N$ is a normal subgroup of $G$, then $N \cap Z(G) = \{e\}$ if and only if $N = \{e\}$. In particular $Z(G) \neq \{e\}$, if $G \neq \{e\}$.

(b) If $|G| = p^2$, then $G$ is abelian and is isomorphic to $\mathbb{Z}_{p^2}$ or to $\mathbb{Z}_p \times \mathbb{Z}_p$.

*Proof.* (a) Since $N$ is normal in $G$ we have by (2.2.4) $N = \bigcap_{i=1}^{s} C_i$ is a disjoint union of some conjugacy classes $C_i$, $i = 1, \cdots, s$ of $G$ contained in $N$. Let $C_1 = \{e\}$. Then $|N| = |N \cap Z(G)| + \sum_{|C_i| > 1} |C_i|$ since a conjugacy class $C_i \subseteq N$ is of length 1 if and only if $C_i \subseteq N \cap Z(G)$. Since $|C_i|$ divides $|G| = p^n$. We get $|N \cap Z(G)| \equiv 0 \pmod{p}$ if and only if $|N| \equiv 0 \pmod{p}$, that is, $N \neq \{e\}$.

Since $|N \cap Z(G)| \geq 1$, we get $N \cap Z(G) = \{e\}$ if and only if $N \neq \{e\}$.

If $G = N$, then we get $Z(G) = \{e\}$ if and only if $G = \{e\}$.

(b) If $|G| = p^2$, we get $Z(G) \neq \{e\}$: We have to show that $Z(G) = G$. If $Z(G) \neq G$ then both $Z(G)$ and $G/Z(G)$ are of order $p$ and hence cyclic, since any group of prime order must be cyclic by Lagrange’s theorem. So $Z(G) = < a >$ and $G/Z(G) = bZ(G) >$ for some $a, b \in G$. Let $g \in G$, then $gZ(G) = b^n Z(G)$ for some $i$ and hence $g \in b^i < a >$. Now $g = b^i a^j$ for some $i$ and $j \in \mathbb{N}$. But then for any $g_1 = b^{i_1} a^{j_1}$ and $g_2 = b^{i_2} a^{j_2}$ in $G$ we have $g_1 g_2 = b^{i_1} a^{j_1} b^{i_2} a^{j_2} = b^{i_1 + i_2} a^{j_1 + j_2} = b^{i_2} b^{i_1} a^{j_2} a^{j_1} = g_2 g_1$ since $a \in Z(G)$ . Thus $G$ is abelian.

**2.3.5. Lemma.** Let $G$ be a group and $U$ and $V$ be subgroups of $G$. Then $\mu : (U \times V) \times G \to G$ given by $\mu((u, v), g) = uv^{-1}$ for any $(u, v) \in U \times V$ and $g \in G$ defines an action of $U \times V$ on $G$. The orbit of $U \times V$ on $G$ containing $g \in G$ is the set $UgV = \{ugv | u \in U, v \in V\}$. If $Y$ is a subset of $G$ containing exactly one element from each orbit, then the disjoint union

$$G = \bigcup_{y \in Y} UgV$$
is called the \textit{decomposition of $G$ into double cosets with respect to $(U,V)$}. Furthermore we have $|UgV| = \frac{|U||V|}{|g^{-1}UgV|}$ if $U$ and $V$ are finite.

\textbf{Proof.} $\mu$ defines an action of the group $U \times V$ on $G$ since

(i) $\mu(e,e,g) = ege^{-1} = g$ for all $g \in G,$ and

(ii) $\mu(u_1,v_1)(u_2,v_2), g) = \mu((u_1u_2,v_1v_2), g) = (u_1u_2)g(v_1v_2)^{-1} = u_1(u_2g)v_2^{-1}v_1^{-1} = \mu((u_1,v_1), u_2g)\mu((u_2,v_2), g)$ for all $(u_1,v_1), (u_2,v_2) \in U \times V$ and all $g \in G.$

The orbit of $U \times V$ on $G$ containing $g \in G$ is $\{\mu(u,v), g]|u \in U, v \in V\} = \{ugv^{-1}|u \in U, v \in V\} = \{ugv|u \in U, v \in V\} = UgV.$

Since multiplication from left is a bijection and hence $|UgV| = |g^{-1}(UgV)|$. Thus if $U$ and $V$ and finite subgroups, we get $|UgV| = |g^{-1}UgV| = \frac{|U||V|}{|g^{-1}UgV|}.$

\textbf{2.3.6. Lemma.} Let $G$ be a group and $H$ a subgroup of $G$. Then $|[gHg^{-1}|g \in G]| = |G : N_G(H)|$ where $N_G(H) = \{g \in G|gHg^{-1} = H\}$ is the normalizer of $H$ in $G$.

\textbf{Proof.} $G$ acts transitively on the set $\{gHg^{-1}|g \in G\}$ by conjugation. The stabilizer of $H \in \{gHg^{-1}|g \in G\}$ in $G$ is $N_G(H)$. Hence by (2.2.1) we have $\{|gHg^{-1}|g \in G\}| = |G : N_G(H)|.$

\textbf{2.3.7. Theorem.} If $G$ is a finite $p$-group and $H$ a proper subgroup of $G$, then $H$ is also a proper subgroup of $N_G(H)$. In particular any maximal subgroup of $G$ is normal in $G$ and has index $p$ in $G$. (Here a subgroup $H$ of a group $G$ is called a \textit{maximal} subgroup if $H \neq G$ and if $H \leq M \leq G$, then $H = M$).

\textbf{Proof.} Consider the double coset decomposition $\bigcap_{i=1}^{k} Hg_iH$ of $G$ with $y_i = e$. Then $|G| = \sum_{i=1}^{k} \frac{|H||H|}{|y_i^{-1}Hg_i \cap H|}$ and hence $|G : H| = 1 + \sum_{i=2}^{k} \frac{|H|}{|y_i^{-1}Hg_i \cap H|} = 1 + \sum_{i=2}^{k} |H : y_i^{-1}Hg_i \cap H|.$ Since $H$ is a proper subgroup of $G$, $p$ divides $|G : H|$. If $(y_i^{-1}Hg_i) \cap H$ were a proper subgroup of $H$, for each $i = 2, \ldots , k$, we would get $p[H : (y_i^{-1}Hg_i) \cap H]$ for all $i = 2, \ldots , k$ and hence the contradiction that $p$ divides $|G : H|$. Thus there exists $i_0 \geq 2$, with $y_{i_0}^{-1}Hg_{i_0} \cap H = H.$
Then \( y^{-1}_o H y_o = H \) and hence \( y_o \in N_G(H) - H \), that is, \( H \) is a proper subgroup of \( N_G(H) \).

In particular if \( H \) is a maximal subgroup, then \( H \not= G \) and hence \( H \not\subseteq N_G(H) \leq G \) and \( N_G(H) = G \) by the maximality of \( H \). Now \( G/H \) is a nontrivial \( p \)-group, and so it has a subgroup of order \( p \), by Cauchy’s theorem, say \( K/H \). Then \( H \not\subseteq K \leq G \) and hence \( K = G \) by the maximality of \( H \). This gives \( |G : H| = p \) \( \square \)

2.3.8. Remark. Not every \( p \)-group has a maximal subgroup. For example \( C_{p^\infty} \) has no maximal subgroups.

2.4. Permutation representations

2.4.1. Theorem. Let \( G \) be a group acting on a nonempty set \( X \). Then, for each \( g \in G \), the map \( \rho_g : X \to X \) defined by \( \rho_g(x) = gx \) is a permutation of \( X \) and the map \( \rho : G \to S_X \) given by \( \rho(g) = \rho_g \) is a homomorphism, which is called a permutation representation of \( G \) on \( X \). The set \( \{ g \in G | \rho_g = id_X \} \) of all elements of \( G \) acting trivially on \( X \), is the kernel of \( \rho \) and hence is a normal subgroup of \( G \) which will sometimes be called the kernel of the action.

**Proof.** By (A.II) we have \( \rho_g(\rho_g^{-1}(x)) = \rho_g(g^{-1}x) = g(g^{-1}x) = (gg^{-1})x = ex = x = id_X(x) \) for all \( x \in X \). Thus \( \rho_g \rho_g^{-1} = id_X \) implying that \( \rho_g \in S_X \).

Let us define \( \rho : G \to S_X \) by \( \rho(g) = \rho_g \). Since \( \rho(g_1g_2)(x) = \rho_{g_1g_2}(x) = (g_1g_2)x = g_1(g_2x) = g_1(\rho_{g_2}(x)) = \rho_{g_1}(\rho_{g_2}(x)) = \rho_{g_1}(\rho_{g_2})(x) = \rho(g_1)(\rho(g_2))(x) \) for all \( x \in X \) by (A.II) we get \( \rho(g_1g_2) = \rho(g_1)\rho(g_2) \) for all \( g_1, g_2 \in G \). Thus \( \rho \) is a homomorphism.

We observe that

\[
\text{Ker } \rho = \{ g \in G | \rho(g) = id_X \} = \{ g \in G | \rho_g(x) = x \text{ for all } x \in X \}
= \{ g \in G | gx = x, \text{ for all } x \in X \} = \bigcap_{x \in G} G_x.
\]

Thus \( \rho \) is a homomorphism from \( G \) into \( S_X \) where \( \text{Ker } \rho \) is a normal subgroup of \( G \) consisting of all elements \( g \in G \) acting trivially on \( X \). \( \square \)

2.4.2. Theorem. Let \( G \) be a group and \( X \) a nonempty set. If \( \rho : G \to S_X \) is a homomorphism from \( G \) into \( S_X \), then the map \( \mu : G \times X \to X \) defined by \( \mu(g, x) = \rho(g)(x) \) for \( g \in G, x \in X \) is an action of \( G \) on \( X \).
Proof. Let \( \rho : G \to S_X \) be a homomorphism. Then \( \rho(e) = id_X \) is the identity permutation on \( X \). Hence \( \mu(e,x) = \rho(e)(x) = id_X(x) = x \) for all \( x \in X \). On the other hand

\[
\mu(g_1g_2, x) = \rho(g_1g_2)(x) = \rho(g_1)(\rho(g_2)(x)) = \rho(g_1)(\mu(g_2, x)) = \mu(g_1, \mu(g_2, x)).
\]

Thus

\[
\mu(g_1g_2, x) = \mu(g_1, \mu(g_2, x)) \quad \text{for all } g_1, g_2 \in G \text{ and all } x \in X,
\]

that is, \( \mu \) is an action of \( G \) on \( X \).

\[\square\]

2.5. More on group actions

2.5.1. Theorem. Let \( G \) be a finite group acting on a finite, nonempty set \( X \). If for any \( g \in G \) we denote by \( \mathcal{X}(g) \), the number of elements of \( \mathcal{X} \) fixed by \( g \), that is, \( \mathcal{X}(g) = |\{x \in X | gx = x\}| \), and if \( t \) denotes the number of orbits of \( G \) on \( X \), then

\[
t = \frac{1}{|G|} \sum_{g \in G} \mathcal{X}(g).
\]

If furthermore \( G \) is transitive on \( X \), that is, \( t = 1 \), then

\[
\frac{1}{|G|} \sum_{g \in G} \mathcal{X}(g)^2 = r
\]

is the number of orbits of the stabilizer \( G_x \) on \( X \).

Proof. Let \( Y = \{(g, x) \in G \times X | gx = x\} \) and \( X_1, X_2, \ldots, X_t \) be the orbits of \( G \) on \( X \). We count the elements of \( Y \) in two ways. First, for a fixed \( g \in G \), there exist \( \mathcal{X}(g) \) elements in \( Y \). Thus \( |Y| = \sum_{g \in G} \mathcal{X}(g) \). Next, for a fixed \( x \in X \), there are \( |G_x| \) elements in \( Y \). Thus \( |Y| = \sum_{x \in X} |G_x| = \sum_{i=1}^{t} \sum_{x \in X_i} |G_x| \). By (2.2.1) we have \( |G_x| = |G_{x_i}| \) for all \( x \in X_i \), where \( x_i \in X_i \). This gives \( \sum_{x \in X_i} |G_x| = |X_i||G_{x_i}| = |G| \) by (2.2.1) and hence

\[
\sum_{g \in G} \mathcal{X}(g) = \sum_{i=1}^{t} |G| = t|G|.
\]

Let now \( t = 1 \). Then all stabilizers \( G_x, x \in X \) are conjugate to each other in \( G \), and therefore the number of orbits of a stabilizer \( G_x \) on \( X \) does not depend on the choice of \( x \in X \). Let \( x \in X \) and let \( Y_1 = \{x\}, Y_2, \ldots, Y_r \) be the orbits of \( G_x \) on \( X \) and let \( Z = \{(g_1, y_1, y_2) \in G \times X \times X | gy_1 = y_1 \text{ and } gy_2 = y_2\} \). We count the elements of \( Z \) in two ways. First, for a fixed \( g_0 \in G \) we have \( \mathcal{X}(g_0)^2 \) elements
in $Z$. Thus $|Z| = \sum_{g \in G} X(g)^2$. Next, for a fixed $y_0 \in X$, the number of elements 
$(g, y_0, y) \in Z$ is equal to the cardinality of the set \{$(g, y) \in G_{y_0} \times X | gy = y$\}. But 
by the first part of the proof, we have $|(g, y) \in G_{y_0} \times X | gy = y| = r|G_{y_0}|$. Thus 
$|Z| = \sum_{x \in X} r|G_x| = r|X||G_x| = r|G|$ and hence 

$$\sum_{g \in G} X(g)^2 = r|G|$$

\[ \square \]

2.5.2. Definition. Let $G$ be a group acting on a set $X$.

(a) $G$ is said to be \textit{k-fold transitive on $X$} if for any two $k$-tuples $(x_1, x_2, \cdots, x_k)$
and $(x'_1, x'_2, \cdots, x'_k)$ of elements of $X$ satisfying $y_i \neq y_j$ for $i \neq j$ there exists $g \in G$
with $gx_i = x'_i$ for all $i = 1, \cdots, k$.

(b) For any nonempty subset $Y$ of $X$ and for any $g \in G$ define $gY := \{gy | y \in Y\} \subseteq X$. A nonempty proper subset $Y$ of $X$ is called an \textit{imprimitivity domain} of $G$ in $X$ if $Y$ contains more than one element and for any $g \in G$ we have $gY = Y$ or $gY \cap Y = \phi$. If $G$ acts nontrivially and nontransitively on $X$, then any orbit of $G$ on $X$ containing more than one element is an imprimitivity domain of $G$. $G$ is said to be \textit{imprimitive} on $X$ if $G$ is transitive on $X$ and there exists an imprimitivity domain of $G$ on $X$. $G$ is called \textit{primitive} if $G$ is transitive on $X$ and if $Y$ is a nonempty subset of $X$ with $gY = Y$ or $gY \cap Y = \phi$ for any $g \in G$ then we have either $Y = X$ or $Y = \{y\}$ for some $y \in X$.

2.5.3. Theorem. Assume that the group $G$ acts transitively on the set $X$ with $|X| > 1$.

(a) Let $Y$ be an imprimitivity domain of $G$ on $X$ and let $H = \{g | gY = Y\} \subseteq G$. Then $H$ is a proper subgroup of $G$. Let $G = \bigcup_{t \in T} tH$ be the decomposition of $G$ into \textit{left cosets of $H$ in $G$}. Then $X = \bigcup_{t \in T} tY$ where $t_1, t_2 \in T$ and $t_1 \neq t_2$ implies that $t_1Y \cap t_2Y = \phi$. In particular we get 

$$|X| = |Y||G : H| \text{ if } |X| < \infty.$$  

(b) Let $N \trianglelefteq G$. If $N$ is not transitive on $X$ and does not act trivially on $X$, 
then the orbits of $N$ are imprimitivity domains of $G$ and are of the same length. 
In particular every nontrivial normal subgroup of a primitive permutation group is 
transitive.
(c) $G$ acts primitively on $X$ if and only if the stabilizer $G_x$, for some (and hence for any) $x \in X$, is a maximal subgroup of $G$, that is, there exists no subgroup $H$ of $G$ with $G_x \not\subseteq H \not\subseteq G$.

Proof. (a) It is easy to check that $H$ is a subgroup of $G$. For any $x \in X$ there exist $y \in Y$ and $g \in G$ with $gy = x$, since $G$ is transitive on $X$. If $g = th \in tH$ with some $h \in H$, then $gy = (th)y = t(hy)$ with $hy \in Y$. Thus $x \in tY$ and hence $X = \bigcup_{t \in T} tY$. Let now $t_1 t_2 \in T$, $t_1 \neq t_2$. If there exists $x \in t_1Y \cap t_2Y$, then $t_1^{-1}, t_2 \in H$, that is, $t_2 \in t_1H$. But this is not possible, since $T$ is a transversal for $H$ in $G$. If $|X|$ is finite, then $|G : H| = |T|$ is finite and we get $|X| = \sum_{t \in T} |tY| = \sum_{t \in T} |Y| = |T| \cdot |Y|$.

(b) Let $Y$ be an orbit of $N$ on $X$ with $|Y| > 1$. There exists such an orbit of $N$, since $N$ does not act trivially on $X$. $Y \neq X$ as $N$ is not transitive on $X$. Let $g \in G$ and assume that $gY \cap Y \neq \phi$. Then there exists $y_1 \in Y$ with $g y_1 \in Y$. Since $N$ is transitive on $Y$ ($Y$ is an orbit of $N$), for any $y \in Y$ we have $n y_1 = y$ for some $n \in N$. Thus $gy = gny_1 = (gn^{-1})gy_1 = m(gy_1)$ where $m = gn^{-1} \in N$ and $gy_1 \in Y$. This gives $gy \in Y$, for any $y \in Y$, that is, $gY \subseteq Y$. On the other hand for any $y \in Y$ we have $s y = g y_1$ for some $s \in N$ since $N$ is transitive on $Y$. Hence $y = g(s^{-1} - 1)g y_1 = gY$, since $g^{-1} - 1 \in N$ and $(g^{-1} - 1)s y_1 \in Y$. Thus $gY = Y$, so $Y$ is an imprimitivity domain for $G$. That the orbits of $N$ on $X$ are of the same length follows then from (a). (Exercise)

In a permutation group $G$ on $X$ any nontrivial subgroup acts nontrivially on $X$. So if $G$ is primitive, any nontrivial normal subgroup $N$ of $G$ must act transitively on $X$ by the above paragraph.

(c) Let $G$ be primitive on $X$. Then $G_2$ is a proper subgroup of $G$ for any $x \in X$, since $|X| > 1$ and $G$ is transitive on $X$. Let now $H$ be a subgroup of $G$ with $G_2 \not\subseteq H$ and let $Y = \{hx | h \in H\}$. Then $\{x\} \not\subseteq Y$ since $G_2 \not\subseteq H$. Let $g \in G$ and assume that $gY \cap Y \neq \phi$. Then there exist $y_1 = h_1 x \in Y$ with $g y_1 = h_2 x \in V$, $h_1, h_2 \in H$. Thus $h_2^{-1}g y_1 x = x = h_2^{-1}gh_1 x$ and hence $h_2^{-1}gh_1 \in G_2 \subseteq H$. This gives $g \in H$ and hence $gY = Y$. Since $G$ is primitive on $X$ we must have $Y = X$ since $|Y| > 1$. But since the elements in $X$ correspond bijectively to the cosets of $G_2$ in $G$, we get $H = G$. 
Conversely let $G_x$ be a maximal subgroup of $G$. If $G$ is not primitive, there exists by (a) an imprimitivity domain $Y$ for $G$ with $x \in Y$. There exists $y \in Y - \{x\}$, since $|Y| > 1$. Since $G$ is transitive on $X$, there exists $g_1 \in G$ with $g_1y = x$. Then $g_1Y \cap Y \neq \phi$ and hence $g_1Y = Y$. Let $H = \{g \in G | gY = Y\}$. Then $G_x \nsubseteq \langle G_x, y \rangle \leq H \leq G$. Thus $H = G$, as $G_x$ is maximal in $G$. But this is not possible since $Y \nsubseteq X$ and $G$ is transitive on $X$.

\[\square\]

2.5.4. Theorem. Let $G$ be a group acting transitively on the set $X$ with $|X| > 1$.

(a) $G$ is doubly transitive on $X$ if and only if $G_x$ acts transitively on $X - \{x\}$, for any $x \in X$.

(b) Let $G = \bigcup_{t \in T} G_x t G_x$ be the double coset decomposition of $G$ by $(G_x, G_x)$, for some $x \in X$. Then the subsets $X_t = \{gx | g \in G_x t G_x\}$, $t \in T$ are the orbits of $G_x$ on $X$. In particular $G$ is doubly transitive on $X$ if and only if $G = G_x \cup G_x gG_x$ for any $g \in G \setminus G_x$.

(c) If $G$ is doubly transitive on $X$, then $G$ is primitive on $X$.

Proof. (a) If $G$ is doubly transitive then for any two points $(x, y_1)$ and $(x, y_2) \in X \times X$ with $y_1 \neq x \neq y_2$ there exists $g \in G$ with $gx = x$ and $gy_1 = y_2$. This means that $G_x$ acts transitively on $X - \{x\}$.

Assume conversely that $G_x$ acts transitively on $X - \{x\}$, for any $x \in X$, and let $(x_1, x_2), (y_1, y_2) \in X \times X$ with $x_1 \neq x_2$ and $y_1 \neq y_2$. If $x_1 = y_1$ or $x_1 = y_2$, then there exists $g \in G_x$, with $gx_2 \in \{y_1, y_2\} - \{x_1\}$ and there is nothing to prove. So we can assume without loss of generality that $\{x_1, x_2\} \cap \{y_1, y_2\} = \phi$. Then there exists $g_1 \in G_x$, with $gx_2 = y_2$ and $g_2 \in G_y$ with $gx_1 = y_1$. Letting $g = g_2g_1$ we get $gx_1 = y_1$ and $gx_2 = y_2$. Thus $G$ is doubly transitive on $X$.

(b) We have $X_t = \{gx | g \in G_x t G_x\} = \{gtx | g \in G_x\}$. Thus $G_x$ is transitive on $X_t$ for any $t \in T$, and $\bigcup_{t \in T} X_t = X$. We need only to show that for distinct $t_1, t_2 \in T$ there exists no $g \in G_x$ with $gt_1x = t_2x$. If this holds we get $(t_2^{-1}g t_1)x = x$ and hence $t_2^{-1}g t_1 \in G_x$. Thus $t_1 \in g^{-1}t_2 G_x \subseteq G_x t_2 G_x$ which implies that $t_1 = t_2$.

In particular $G$ is doubly transitive on $X$ if and only if $G_x$ has exactly two orbits on $X$, namely $\{x\}$ and $X - \{x\}$, and this holds if and only if $|T| = 2$ by the above paragraph.
(c) Let $G$ be doubly transitive on $X$. Let $Y$ be a subset of $X$ with $|Y| \geq 2$ and let $x \in Y$. Then for any $z \in X - \{x\}$ there exists $y \in Y - \{x\}$ and $g \in G_x$ with $gy = z$. Thus $X \subseteq gY$ and hence $G$ cannot have any imprimitivity domain on $X$. Thus $G$ is primitive on $X$. 

Exercises

1) Let $G$ be a finite group and $H$ a subgroup of $G$ with $|G : H| = p$, where $p$ is the smallest prime dividing the order of $G$. Then $H \trianglelefteq G$.

2) Let $G$ be a finite group of order $|G| = 2^n q$ where $q$ is odd. Assume that $G$ has an element of order $2^n$. Then $G$ has a normal subgroup of order $q$.

(Hint: Let $g \in G$ with $o(g) = 2^n$ and compute $\text{sign}(g)$, where $\alpha$ is the regular permutation representation of $G$, to show that $G$ has a normal subgroup $K$ of order $2^{n-1}q$, containing an element of order $2^{n-1}$. Apply induction on $n$.)

3) Let $G$ be a group of order 15. Show that $G$ is cyclic.

4) Let $\alpha$ be an automorphism of the finite group $G$ such that $\alpha(g)$ is conjugate to $g$ in $G$, for any $g \in G$. Then every prime divisor of $o(\alpha)$ divides also $|G|$.

(Hint: Without loss of generality, one can assume that $o(\alpha) = p$, $p$ a prime not dividing $|G|$ and try to get a contradiction. $\alpha$ acts on each conjugacy class $C$ of $G$. \{g \in G|\alpha(g) = g\} = H$ is a proper subgroup of $G$ and $H \cap C \neq \emptyset$ for each conjugacy class $C$ of $G$. Consider $\bigcup_{g \in G} gHg^{-1}$.)

Is such an automorphism $\alpha$ of $G$ necessarily an inner automorphism?

5) (a) If $G$ is a group and $G/Z(G)$ is cyclic, then $G$ is abelian.

(b) If $G$ is a nonabelian finite $p$-group, then $p^2$ divides $|G : Z(G)|$. In particular any group of order $p^2$ is abelian.

(c) If $G$ is a finite $p$-group with $|G| \geq p^2$, then $|C_G(x)| \geq p^2$ for any $x \in G$.

6) (a) Let $\gamma = (1, 2, \cdots, n) \in S_n$. Find the length of the conjugacy class of $\gamma$ in $S_n$. Find $C_{S_n}(\gamma)$. 


(b) Let \( \alpha \in S_n \) be of type \( (z_1, z_1, \ldots, z_1; z_2, z_2, \ldots, z_2; \ldots; z_s, z_s, \ldots, z_s) \)
\( n_1 \)-times \( n_2 \)-times \( n_3 \)-times
where \( \sum_{i=1}^{s} n_i z_i = n \), \( z_1 > z_1 > \cdots > z_s \). Show that the number of elements in \( S_n \) conjugate to \( \alpha \) is

\[
n! \prod_{i=1}^{s} n_i! \prod_{i=1}^{s} z_i^{n_i}.
\]

7) If there are \( q \) colors available, prove that there are \( \frac{1}{n} \sum_{d \mid n} \varphi\left(\frac{n}{d}\right) q^d \) colored roulette wheels having \( n \) equal compartments, where \( \varphi \) is the Euler \( \varphi \)-function.

(Hint: Let \( X \) be the set of all ordered sets of \( n \) colored boxes and let \( G = \langle (1, 2, \ldots, n) \rangle \) act on \( X \) by \( \langle q_1, q_2, \ldots, q_n \rangle \mapsto q_2, q_3, \ldots, q_n, q_1 \rangle \). Then a colored roulette wheel corresponds to an orbit of \( G \) on \( X \). Apply (2.18). Let \( \alpha = (1, 2, \ldots, n) \) and \( \chi(\alpha^k) \) be the number of fixed points of \( \alpha^k \) on \( X \). Using Exercise (13,f) of Chapter I show that \( \chi(\alpha^k) = q^{(n, k)} \).)

8) Let \( G \) be a finite subgroup of \( GL(3, \mathbb{R}) \) consisting of rotations. Every element \( g \in G - \{ e \} \) determines two points on the unit sphere in \( \mathbb{R}^3 \), namely the intersection points of the axis of \( g \) with the unit sphere. These are the only points of the sphere which are fixed by \( g \in G - \{ e \} \), and are called the poles of \( g \). Let \( P = \{ x \in \mathbb{R}^3 \mid |x| = 1, gx = x, \text{ for some } g \in G - \{ e \} \} \) be the set of poles of elements of \( G - \{ e \} \). Show that the natural action of \( GL(3, \mathbb{R}) \) on \( \mathbb{R}^3 \) induces an action of \( G \) on \( P \). Let \( P_1, P_2, \ldots, P_k \) be the orbits of \( G \) on \( P \). Applying (2.18) show that \( k = \sum_{i=1}^{k} \frac{|P_i|}{|G|} + 2(1 - \frac{1}{|G|}) \). Deduce that either \( k = 2 \) or \( k = 3 \).

If \( k = 2 \), then \( |P_1| = |P_2| = 1 \) and hence every \( g \in G - \{ e \} \) has the same axis. Show that \( G \) is a cyclic group in this case.

If \( k = 3 \) then we get \( \frac{|P_1|}{|G|} + \frac{|P_2|}{|G|} + \frac{|P_3|}{|G|} = 1 + \frac{2}{|G|} \), with \( \frac{|P_4|}{|G|} < 1 \).

Then we have with a suitable numbering of the orbits:

1. \( |P_1| = |P_2| = \frac{|G|}{2} \) and \( |P_3| = 2 \)
2. \( |G| = 12 \) and \( |P_1| = G, |P_2| = |P_3| = 4 \)
3. \( |G| = 24 \) and \( |P_1| = 12, |P_2| = 8, |P_3| = 6 \)
4. \( |G| = 60 \) and \( |P_1| = 30, |P_2| = 20, |P_3| = 12 \).
Furthermore $G$ is isomorphic to a dihedral group in (1), to $A_4$ in (2), to $S_4$ in (3) and to $A_5$ in (4).

9) Let $P = \{1, 2, 3, 4, 5, 6, 7\}$ and $L = \{L_i | i = 1, 2, \ldots, 7\}$ with $L_1 = \{1, 2, 3\}, L_2 = \{1, 5, 6\}, L_3 = \{1, 3, 7\}, L_4 = \{2, 6, 7\}, L_5 = \{2, 3, 5\}, L_6 = \{3, 4, 6\}, L_7 = \{4, 5, 7\}$. The incidence structure consisting of the points (!) $x \in P$ and the lines (!) $L \in L$ with the incidence relation $x \in L$ is a finite projective plane of order $q = 2$, that is, the following conditions are satisfied:

(i) For any two distinct points $x_1, x_2 \in P$ there exists a unique line $L \in L$ with $x_1 \in L$ and $x_2 \in L$.

(ii) For any two distinct lines $L_{(1)}$ and $L_{(2)}$ in $L$ there exists a unique point $x \in P$ with $x \in L_{(1)}$ and $x \in L_{(2)}$.

(iii) There exists four points determining two by two six distinct lines.

(iv) There exists a line which consists of $q + 1 (= 3)$ points.

An automorphism of this structure is a permutation $\alpha$ in $S_p$ such that for any $L \in L$ we have $\alpha(L) = \{\alpha(x) | x \in L\} \in L$. The set of all automorphisms of this structure is a subgroup $G$ of $S_p$ and acts in a natural way both on $P$ and on $L$.

Show that

a) $\alpha = (1234567) \in G$, hence $G$ is transitive on $P$.

b) $\beta = (235)(476) \in G$. $G$ is doubly transitive on $P$.

c) Using $|P| = |G : G_1|$ and $|P - \{1\}| = |G_1 : G_{1,2}|$ and determining $G_{1,2} = \{g \in G | g_1 = 1 \text{ and } g_2 = 2\}$, show that $|G| = 168$.

d) Is the permutation representation of $G$ on $P$ equivalent to the permutation representation of $G$ on $L$?

(After /s 3) Show that $G$ is simple

(Hint: Let $\{e\} \neq N \leq G$. Then $N$ is transitive on $P$ and so 7 divides $|N|$.

(i) $|N| \neq 7$. Otherwise $G/C_G(N)$ is isomorphic to a subgroup of Aut $N$. Deduce that there exists $g \in C_G(N)$ with $o(g) = 2$. How does $N$ act on $\{x \in P | gx = x\}$?

(ii) By (i) the number of Sylow 7-subgroups of $N$ is 8. If $|N| = 7.8$, then there exist $(7 - 1) \cdot 8 = 48$ elements of order 7 in $N$. So a Sylow 2-subgroup $T$ of $N$ is normal in $N \cdot X = \{x \in P | gx = x \text{ for all } g \in T\} \neq \phi$ and a Sylow
7-subgroup of \(N\) acts on \(X\). Conclude that \(N = G\).)

10) Prove: If \(G\) is a finite group of order \(|G| = p^n \cdot m\) with \(p\) a prime not dividing \(m\), then \(G\) has a subgroup of order \(p^n\).

(Hint: Let \(G\) be a minimal counter example Then \(G\) is not a \(p\)-group. By \((2.10)\) there exists a subgroup \(H \leq G\) with \(|H| = q\), where \(q\) is a prime different from \(p\). Let \(X = \{T|T \text{ a left transversal for } H \text{ in } G\}\) Then \(|X| = q^{[G:H]}\) and \(G\) acts on \(X\) by multiplication from left. There exists an orbit \(Y\) of \(G\) on \(X\) such that \(|Y|\) is not divisible by \(p\). If \(T \in Y\), let \(K = G_T\) be the stabilizer of \(T\) in \(G\). Compute \(|G_T|\) and use \(|G_T| < |G|\).

11) Let the group \(G\) act on the set \(X\) transitively. Then the action of \(G\) on \(X\) is equivalent to the action of \(G\) on the left cosets of the stabilizer \(G_x\) for some \(x \in X\), by multiplication from left.

12) Let \(A \leq \text{Aut}\, G\), \(G\) a finite group. Then \(A\) acts on \(G\) by \((\alpha, g) \mapsto \alpha(g)\).

\(a)\) If \(A\) acts transitively on \(G - \{e\}\), then \(G\) is elementary abelian for some prime \(p\).

(Hint: First show that every element of \(G - \{e\}\) is of order \(p\). So \(G\) is a \(p\)-group and \(Z(G) \neq \{e\}\). Show that for any \(\alpha \in A\), \(\alpha(Z(G)) = Z(G)\) and hence \(Z(G) = G\).

\(b)\) If \(A\) acts 2-fold transitively on \(G - \{e\}\), then either \(p = 2\) or \(|G| = 3\).

(Hint: \(A\) is primitive on \(G - \{e\}\). Let \(g \in G - \{e\}\) and \(Y = \{g, g^{-1}\}\). If \(\alpha \in \text{Aut}\, A\) and \(\alpha(Y) \cap Y \neq \phi\), then \(\alpha(Y) = Y\). Hence \(|Y| = 1\) or \(Y = G - \{e\}\).)

\(c)\) If \(A\) acts 3-fold transitively on \(G - \{e\}\), then either \(|G| = 3\) or \(|G| = 4\).

13) Let \(G \leq S_x\) and assume that \(G\) acts transitively on \(X\). Let \(N\) be a regular normal subgroup \(G\), that is, \(N\) is transitive on \(X\) and no element of \(N - \{e\}\) fixes any element of \(X\) and \(N \leq G\). For a fixed \(x \in X\) and any \(y \in X\), there exists a unique \(n \in N\) with \(nx = y\). \(G_x\) acts on \(N\) by conjugation in such a way that \(gng^{-1}\) is the unique element of \(N\) which maps \(x\) to \(gy\), if \(n \in N\) with \(nx = y\) and \(g \in G_x\). The action of \(G_x\) on \(X - \{x\}\) and the above action of \(G_x\) on \(N - \{e\}\) by conjugation are equivalent. In particular \(G\) acts \(k\)-fold transitively on \(X\) (if and only if \(G_x\) acts \((k-1)\)-fold transitively
on $X \setminus \{x\}$ if and only if $G_x$ acts $(k - 1)$-fold transitively on $N \setminus \{e\}$ by conjugation.

14) Prove that $A_n$ is simple for all $n \neq 4$.
(Hint: Without loss of generality $n \geq 5$. By induction on $n$, $A_5$ simple, $n \geq 6$.
   a) $A_n$ is $(n - 2)$-fold transitive on $\{1, 2, \cdots, n\}$. (Exercise 13.c of Chapter I)
   b) Let $\{e\} \neq N \unlhd A_n$ and identify $A_{n-1}$ with $\{g \in A_n | g(1) = 1\} = (A_n)_1$.
      Since $N \cap A_{n-1} \leq A_{n-1}$ we have $N \cap A_{n-1} = \{e\}$ or $N \cap A_{n-1} = A_{n-1}$.
      Since $N$ transitive on $\{1, \cdots, n\}$, $N \cap A_{n-1} = A_{n-1}$ implies that $N = A_n$.
   c) If $N \cap A_{n-1} = \{e\}$, $N$ is a regular normal subgroup of $A_n$. By Exercise 13, $A_{n-1}$ acts $(n - 3)$-fold transitively on $N = \{e\}$. By Exercise 12.c we get $n = |N| = 3$ or $4$, a contradiction).

15) a) Let $G$ be a group acting transitively on the set $X$. Then $N_G(G_x)$ acts transitively on $Y = \{y \in X|gy = y, \text{ for all } g \in G_x\}$.
   b) Every abelian, transitive permutation group $G \leq S_X$ is regular, and $C_{S_X}(G) = G$
   c) A transitive group of prime degree is primitive.
   d) Let $G \leq S_X$, $|X| < \infty$. Suppose that $G$ contains a minimal normal subgroup $N \neq \{e\}$, which is transitive and abelian. Then $G$ is primitive.
CHAPTER III

Sylow Theorems

We have seen that $A_4$ has no subgroups of order 6. So in a finite group the converse of the Lagrange’s Theorem does not necessarily hold. So one can ask, whether the class of finite groups for which the converse of Lagrange’s theorem holds, can be characterized by some interesting structural properties. And further one can ask, whether there exists some distinguished divisors $n \in \mathbb{N}$ such that any group $G$ whose order is divisible by $n$ has subgroups of order $n$. This chapter is devoted to the second question. The results we shall obtain in this chapter are among the most important, and beautiful theorems in the theory of finite groups.

3.1. Theorem. Let $G$ be a finite group of order $|G| = p^k m$ where $p$ is a prime. Then the number of subgroups of $G$ of order $p^k$ is congruent to 1 modulo $p$.

Proof. (Wielandt). Let $X = \{ M | M \subseteq G, |M| = p^k \}$ be the set of all subsets of $G$ containing exactly $p^k$ elements $|X| = \binom{p^k m}{p^k}$. $G$ acts on $X$ by multiplication from left : $(g, M) \rightarrow gM = \{ gm | m \in M \} \in X$. Let $X_1, X_2, \ldots, X_r$ be the orbits of $G$ on $X$. Let $M_i \in X_i$ and $G_i$ the stabilizer of $M_i$ in $G(i = 1, \ldots, r)$. Then we have by \( \left( \begin{array}{c} p^k m \\ p^k \end{array} \right) \) $|X| = \sum_{i=1}^{r} |X_i| = \sum_{i=1}^{r} |G : G_i|$. That $G_i$ is the stabilizer of $M_i$ means that $G_i M_i = M_i$, and this says that $M_i$ is the disjoint union of some cosets of $G_i$ contained in the set $M_i$. Thus $M_i = \sum_{j=1}^{s_i} G_i m_{ij}$, with $m_{ij} \in M_i$, $i = 1, 2, \ldots, r$. We get $|M_i| = |G_i| \cdot s_i$, and hence $|G_i| = p^{a_i} \leq p^k$. This gives 

\[ \left( \begin{array}{c} p^k m \\ p^k \end{array} \right) = |X| = \sum_{i=1}^{r} |X_i| = \sum_{|X_i| = m} |X_i| \pmod{(pm)}. \]

Next we show that any orbit $X_i$ of $G$ on $X$ of length $m$ is the set of all cosets of a unique subgroup $H$ of $G$ of order $p^k$. Let $H$ be a subgroup of $G$ of order $p^k$. Then $\{ gH | g \in G \}$ is obviously an orbit of $G$ on $X$ with of length $m$. If $H_1$ and $H_2$ are two different subgroups of $G$ of order $p^k$, then the corresponding orbits of $G$ on $X$ given as $\{ gH_1 | g \in G \}$ and $\{ gH_2 | g \in G \}$ are distinct since $g_1 H_1 = g_2 H_2$ for some $g_1, g_2 \in G$ implies that $g_2^{-1} g_1 H_1 = H_2$ and hence $g_2^{-1} g_1 \in H_2 \iff g_1 H_1 = g_2 H_2$, implying $g_1 H_1 = g_1 H_2$ and hence $H_1 = H_2$. Now conversely let $X_i$ be an orbit of $G$ on $X$ with $|X_i| = m$. Let $M \in X_i$ and $H$ the stabilizer of $M$. Then $|G : H| = m$ and hence $|H| = p^k$. This gives that $Hm = M$ for some $m$ by the
observation in the first paragraph. Then $m^{-1}Hm$ is a subgroup of $G$ of order $p^k$ and $m^{-1}Hm = mM \in X_i$ since $X_i$ is an orbit of $G$ on $X$ and $m^{-1}Hm \in M_i$ we get that $X_i = \{g(m^{-1}Hm)|g \in G\}$.

So if $n$ denotes the number of subgroups of $G$ of order $p^k$, we get that

\[
\left( \frac{p^km}{p^k} \right) \equiv n \cdot m \pmod{pm}
\]

This holds in any group of order $p^km$. It holds in particular in the cyclic group of order $p^km$. Since it has only one subgroup of order $p^k$ we must have

\[
\left( \frac{p^km}{p^k} \right) \equiv m \pmod{pm}
\]

Combining these two results we get $m \equiv mn \pmod{pm}$ and hence $n \equiv 1 \pmod{p}$.

\[\square\]

3.2. Remark. Let $G$ be a group of order $p^n m$ where $p$ is a prime not dividing $m$. Then $G$ has subgroups of order $p^n$ by (3.1). These subgroups are called Sylow $p$-subgroups of $G$. The set of all Sylow $p$-subgroups of $G$ will be denoted by

\[Syl_p G = \{H|H \leq G, \ |H| = p^n, \ (|G:H||,|H|) = 1\}.\]

3.3. Theorem. (Sylow) Every finite group $G$ has Sylow $p$-subgroups. The number $n_p$ of Sylow $p$-subgroups of $G$ is congruent to 1 modulo $p$.

3.4. Theorem. (Sylow) Let $G$ be a finite group.

a) If $H$ is a subgroup of $G$ with $|H| = p^k$ for some prime $p$, then there exists a Sylow $p$-subgroup $P$ of $G$ and $g \in G$ with $H^g = gHg^{-1} \leq P$.

b) All Sylow $p$-subgroups of $G$ are conjugate to each other in $G$. If $P$ is a Sylow $p$-subgroup of $G$, then $|G : N_G(P)| \equiv 1 \pmod{p}$.

Proof. a) Let $H \leq G$ with $|H| = p^k$ and $P \in Syl_p G$. Consider the double coset decomposition of $G$ with respect to $H$ and $P$, $G = \bigcup_{i=1}^r Hx_i P$, $x_1 = e$. Then

\[|G| = \sum_{i=1}^r |P| \cdot \frac{|x_i^{-1}Hx_i|}{|x_i^{-1}Hx_i \cap P|} \quad \text{and hence} \quad |G : P| = \sum_{i=1}^r |x_i^{-1}Hx_i : (x_i^{-1}Hx_i) \cap P|.
\]

For each $i = 1, \cdots, r$ $|x_i^{-1}Hx_i : (x_i^{-1}Hx_i) \cap P|$ divides $|H| = p^k$. If there exists no $i \in \{1, \cdots, r\}$ with $|x_i^{-1}Hx_i : (x_i^{-1}Hx_i)P| = 1$ then we get $p$ divides $|G : P|$. But this is not possible since $P$ is a Sylow $p$-subgroup of $G$. Thus there exists $i_0 \in \{1, \cdots, r\}$ with $|x_{i_0}^{-1}Hx_{i_0} : (x_{i_0}^{-1}Hx_{i_0}) \cap P| = 1$, that is, $x_{i_0}^{-1}Hx_{i_0} = x_{i_0}^{-1}Hx_{i_0} \cap P$ and hence $gHg^{-1} \leq P$ with $g = x_{i_0}^{-1}$.
Proof. For any $H \in Syl_pG$, there exists a $P \in Syl_pG$ such that $H^g \leq P$ for some $g \in G$, by (a). Since $|H^g| = |P| < \infty$, we get $H^g = P$. So the number of Sylow $p$-subgroups of $G$ is then equal to $|G : N_G(P)|$ by (3.3) and hence (3.3) gives that $|G : N_G(P)| \equiv 1 \pmod{p}$.

3.5. Theorem. Let $P$ be a Sylow $p$-subgroup of the finite group $G$ and $N \leq G$. Then

(a) $P \cap N$ is a Sylow $p$-subgroup of $N$.

(b) $PN/N$ is a Sylow $p$-subgroup of $G/N$.

(c) $N_{G/N}(PN/N) = N_G(PN/N)$.

Proof. (a) $P \cap K$ is a subgroup of $P$ and hence is a $p$-group. On the other hand

$|N : N \cap P| = |PN : P|$ and $|PN : P|$ divides $[G : P]$ by $([G : P] = |G : PN| |PN : P|)$ since $PN$ is a subgroup of $G$. As $([G, P], p) = 1$ we get $([N : P \cap N], |P \cap N|) = 1$ and hence $P \cap N \in Syl_pN$.

(b) $|G : PN/N| = |G : PN|$ is prime to $p$ and $PN/N(\equiv P/P \cap N)$ is a $p$-group. Thus $PN/N \in Syl_pG/N$.

(c) Obviously $N_G(P)N/N \leq N_{G/N}(PN/N)$. Let $xN \leq N_{G/N}(PN/N)$.

Then $x^{-1}(PN)x = PN$ and hence $(x^{-1}PN)N = PN$. Thus $x^{-1}Px$ and $P$ are two Sylow $p$-subgroups of $PN$. So by (3.4.b) there exists $y \in P$ and $k \in N$ that is, $x^{-1}Px = k^{-1}y^{-1}P_{yk} = k^{-1}Pk$. We get $xk^{-1} \in N_G(P)$ and hence $x \in N_G(P)N$.

3.6. Theorem. (Frattini Argument) Let $G$ be a finite group and $N$ a normal subgroup of $G$. If $P$ is a Sylow $p$-subgroup of $N$, then $N_G(P)N = G$.

Proof. Let $g \in G$. Then $P^g \leq N^g = N$. Thus $P^g$ and $P$ are two Sylow $p$-subgroups of $N$. So there exists $k \in N$ with $P^g = P^k$ by (3.4.b). This gives $gk^{-1} \in N_G(P)$ and hence $g \in N_G(P)N$.

3.7. Theorem. Let $P$ be a Sylow $p$-subgroup of $G$ and $N_G(P) \leq H \leq G$, then $N_G(H) = H$.

Proof. $p \leq N_G(P) \leq H \leq N_G(H)$. Thus by (3.6) $N_G(H) = N_G(P)$. $H = H$. 

3.8. Theorem. Let $p$ and $q$ be primes with $p > q$ and $G$ be a group of order $|G| = pq$. Then

(a) $G$ has a normal Sylow $P$-subgroup.

(b) If $q$ does not divide $p - 1$, then $G$ is cyclic.

Proof. a) Let $P \in Syl_p G$. Since $P \leq N_G(P)$ we have $|G : N_G(P)|/|G : P| = q$ and $|G : N_G(P)| \equiv 1 \pmod{p}$ by (3.4.b). This forces $|G : N_G(P)| = 1$, that is, $P \leq G$.

b) Let $Q \in Syl_q G$. Then $PQ$ is a subgroup of $G$ of order $|PQ| = |P|/|Q| = pq$, that is, $G = PQ$. If $Q \leq G$, then $P \cap Q = \{e\}$ implies that $G \cong P \times Q$ and since $P$ and $Q$ are cyclic groups we get $G$ is cyclic generated by $x y$ where $P = \langle x \rangle$ and $Q = \langle y \rangle$. If $Q \not\leq G$, then $1 \neq |G : N_G(Q)| \equiv 1 \pmod{q}$ implies that $|G : N_G(Q)| = p = 1 + k q$ for some $k \in \mathbb{N}$. Thus $q$ divides $p - 1$.

\[\square\]

3.9. Theorem. If $G$ is a simple group of order $60 = 2^2 \cdot 3 \cdot 5$. Then $G \cong A_5$.

Proof. Let $n_p$ be the number of Sylow $p$-subgroups of $G$. We have $n_5|12$ and $1 < n_5$ and $n_5 \equiv 1 \pmod{5}$ and hence $n_5 = 6$,

$n_3|20$ and $1 < n_3$ and $n_3 \equiv 1 \pmod{3}$ and hence $n_3 \in \{4, 10\}$,

$n_2|15$ and $1 < n_2$ and $n_2 \equiv 1 \pmod{2}$ and hence $n_2 \in \{3, 5, 15\}$.

Next we observe that $G$ does not contain any proper subgroup $H$ with $|G : H| \leq 5$. If $H \leq G$ and $1 < |G : H| \leq 4$, then $G$ has a normal subgroup $N$ with $N \leq H$ and $|G/N|$ divides $4!$ by (3.2). Thus $N \neq 1$ contradicting the simplicity of $G$. If $H \leq G$ and $|G : H| = 5$, then the permutation representation $\rho$ of $G$ on the cosets of $H$ in $G$ gives a monomorphism of $G$ into $S_5$ (since $G$ is simple). Thus $\rho(G)$ has index 2 in $S_5$ and hence $\rho(G) \leq S_5$. Then $\rho(G)$. $A_5$ is a subgroup of $S_5$ of order $|\rho(G)|$. $|A_5|/|\rho(G) \cap A_5|$. Thus either $\rho(G) \cap A_5 = A_5$ in which case $P(G) = A_5$ and hence $G \cong A_5$ or $|A_5 : \rho(G) \cap A_5| = 2$. But in the second case $1 \neq \rho(G) \cap A_5 \not\leq A_5$ contradicting the simplicity of $A_5$. Thus without loss of generality we can assume that for any proper subgroup $H$ of $G$ we have $|G : H| \geq 5$. This gives $n_3 = 10$ and $n_2 = 15$.

Now let $T_1, T_2 \in Syl_2 G$ and $T_1 \neq T_2$ be chosen such that $|T_1 \cap T_2|$ is maximal. Assume that $T_1 \cap T_2 = D \neq \{e\}$. Then $|D| = 2$ and $D \leq T_1$ and $D \leq T_2$. Let $S = N_G(D)$. Then $S$ contains two different Sylow 2-subgroups, namely $T_1$ and $T_2$. So $S$ contains at least 3 Sylow 2-subgroups since $|Syl_2 S|$ is odd. Thus $12 \not\leq |S|$. Since $S$ is a proper subgroup of $G$, and $G$ is simple, we get $1 \neq |G : S| \leq 5$, which
is not possible. So \( D = \{1\} \), that is, any two distinct Sylow 2-subgroups intersect trivially. Now there are

15. \((4-1) = 45\) elements in \( G \) of order a power of 2.

6. \((5-1) = 24\) elements in \( G \) of order 5.

since any two distinct Sylow 5-subgroups intersect trivially also. So \( G \) contains at least \( 1 + 24 + 45 > 60 \) elements. This is a contradiction. Thus \( G \) is isomorphic to \( A_5 \). □

3.10. Theorem. Let \( K \) and \( L \) be nonempty subsets of a Sylow \( p \)-subgroup \( P \) of the group \( G \), such that \( K^x = K \) and \( L^x = L \) for all \( x \in P \). If there exists \( g \in G \) with \( K^g = L \), then there exists \( y \in N_G(P) \) with \( K^y = L \).

Proof. If \( K^g = L \), then \( N_G(K)^g = N_G(L) \), where \( N_G(K) \) and \( N_G(L) \) are subgroups of \( G \). By assumption, \( p \leq N_G(K) \) and \( p \leq N_G(L) \). Thus \( P^g \leq N_G(K)^g = N_G(L) \) and hence \( P \) and \( P^g \) are two Sylow \( p \)-subgroups of \( N_G(L) \). So there exists \( x \in N_G(L) \) with \( x(gP^{-1}g^{-1}x-1 = P \) by (3.4.b). But then \( xg \in N_G(P) \) and \( K^{yg} = xgKg^{-1}x^{-1} = xLx^{-1} = L \). Let \( y = xg \). □

3.11. Definition. A finite group \( G \) is called nilpotent if \( G \) has exactly one Sylow \( p \)-subgroup for each prime \( p \). By Sylow’s theorem this is equivalent to require that each Sylow \( p \)-subgroup of \( G \) is normal in \( G \) for each prime \( p \).

In the following part of this chapter all groups considered are assumed to be of finite order unless the contrary is stated explicitly.

3.12. Theorem. (a) Any abelian group \( G \) is nilpotent.

(b) If \( G \) is nilpotent and \( H \leq G \), then \( H \) is nilpotent.

(c) If \( G \) is nilpotent, and \( N \unlhd G \), then \( G/N \) is nilpotent.

(d) If \( G_1 \) and \( G_2 \) are nilpotent, then \( G_1 \times G_2 \) is nilpotent.

(e) If \( N \) and \( M \) are normal subgroups of \( G \) and \( G/N \) and \( G/M \) are nilpotent, then \( G/N \cap M \) is also nilpotent.

(f) If \( N \unlhd G \) and \( N \) nilpotent and \( G/N \) nilpotent, does not imply \( G \) to be nilpotent.

(g) If \( G/Z(G) \) is nilpotent, then \( G \) is nilpotent.

Proof. (a) Every subgroup of an abelian group \( G \) is normal.

(b) Let \( P \in Syl_pG \). Then \( P \unlhd G \), since \( G \) is nilpotent. Then \( HP \) is a subgroup of \( G \) and we have \(|HP : P| = 1\), since \(|HP : P|\) divides \(|G : P|\). As \(|HP : P| = \)
\[ H : H \cap P \] we get \( H \cap P \in Syl_p H \). Obviously \( H \cap P \leq H \). This holds for any prime \( p \). Thus \( H \) is nilpotent.

(c) Let \( P \in Syl_p G \). Then \( NP/N \in Syl_p G/N \). Hence if \( P \leq G \), then \( NP \leq G \) and hence \( NP/N \leq G/N \). This yields that the nilpotency of \( G \) implies the nilpotency of any homomorphic image of \( G \).

(d) Any Sylow \( p \)-subgroup of \( G_1 \times G_2 \) is of the form \( P_1 \times P_2 \) where \( P_i \) is a Sylow \( p \)-subgroup of \( G_i \), \( i = 1, 2 \). If \( P_i \leq G_i \), then \( P_i \leq G_1 \times G_2 \), similarly for \( P_2 \). Thus if \( G_1 \) and \( G_2 \) are nilpotent, then so is \( G_1 \times G_2 \).

(e) Let \( \alpha : G \to (G/N) \times (G/M) \) be defined by \( \alpha(g) = (gN, gM) \). \( \alpha \) is a homomorphism with \( \ker \alpha = \{ g \in G | (gN, gM) = (N, M) \} = \{ g \in G | g \in N \cap M \} = N \cap M \). Thus \( G/N \cap M \) is isomorphic to a subgroup of \((G/N) \times (G/M)\). By (d) and (c) the assertion follows.

(f) \( S_3 \) is a group with an abelian normal subgroup \( A_3 \) such that \( S_3/A_3 \) is also abelian. But \( S_3 \) is not nilpotent, since a Sylow 2-subgroup of \( S_3 \) is not normal. (A nilpotent group with abelian Sylow subgroups must be abelian.)

(g) Let \( G/Z(G) \) be nilpotent and let \( P \in Syl_p G \). Then \( Z(G)P/Z(G) \in Syl_p G/Z(G) \) and hence \( Z(G)P/Z(G) \leq G/Z(G) \) by our assumption. This gives \( Z(G)P \leq G \).

By Frattini argument we get \( G = Z(G)PN_G(P) \). But obviously \( Z(G)P \leq N_G(P) \). This yields \( G = N_G(P) \), that is, \( P \leq G \). Thus \( G \) is nilpotent. \( \square \)

3.13. Proposition. The following are equivalent:

(a) \( G \) is nilpotent

(b) \( G \) is direct product of its Sylow subgroups.

(c) If \( H \not\leq G \), then \( H \not\leq N_G(H) \)

(d) If \( H \) is a maximal subgroup of \( G \), then \( H \triangleleft G \).

(e) If \( N \not\leq G \), then \( Z(G/N) \neq \{N\} \).

(f) If \( x, y \in G \) and \( (\sigma(x), \sigma(y)) = 1 \), then \( xy = yx \).

Proof. (a) \( \Rightarrow \) (b) Let \( G \) be nilpotent, of order \( |G| = \prod_{i=1}^{n} p_i^{r_i} \) with distinct primes \( p_i \), \( i = 1, \cdots, n \), and let \( P_i \in Syl_{p_i} G \).

Then \( P_i \leq G, i = 1, \cdots, n \). For \( i, j \in \{1, \cdots, n\} \) with \( i \neq j \) we have \( P_i \cap P_j = \{e\} \) since the order of an element of \( P_i \cap P_j \) must be a power of \( p_i \) and \( p_j \) at the same time for distinct primes \( p_i, p_j \). Then for any \( x \in P_i \) and any \( y \in P_j \) we have \( y = xy \) if \( i \neq j \) (by 1.17). Let now \( g = g_1 g_2, \cdots, g_k \in P_1 P_2 \cdots P_k \cap P_{k+1} \), with
\( g_i \in P_i, i = 1, \ldots, k \). Then \( g^{[P_i]} = \prod_{i=1}^{k} g_i^{[P_i]} = e \) and \( g^{[P_{k+1}]} = e \). Since \((|P_1| \cdots |P_k|, |P_{k+1}|) = 1\) we get \( g = e \) and hence \( P_1P_2 \cdots P_k \cap P_{k+1} = \{e\} \), for any \( k = 1, \ldots, n-1 \). In particular \( |P_1 \cdots P_n| = \prod_{i=1}^{n} |P_i| = |G| \) and thus \( G = P_1P_2 \cdots P_n \).

This gives by (1.22) that \( G = P_1 \times P_2 \times \cdots \times P_n \).

(b) \( \Rightarrow \) (a) If \( G = P_1 \times P_2 \times \cdots \times P_n \) with \( P_i \in \text{Syl}_{p_i} G, i = 1, \ldots, r \), then \( P_i \neq P_j \) and \( P_i \not\trianglelefteq G \), thus \( G \) is nilpotent

(a) \( \Rightarrow \) (c) Let \( G \) be nilpotent and \( H \not\leq G \). Then \( G = P_1 \times P_2 \times \cdots \times P_n \) with \( P_i \in \text{Syl}_{p_i} G \) and \( H = (H \cap P_1) \times (M \cap P_2) \times \cdots (H \cap P_n) \) by (3.12b).

Since \( H \neq G \), there exist an \( i \in \{1, \ldots, n\} \) with \( H \cap P_i \neq P_i \). Then by (2) \( N_{p_i}(H \cap P_i) \not\leq H \cap P_i \). Since \( P_i \) centralizes \( P_j \) for all \( j \in \{1, 2, \ldots, n\} - \{i\} \) we get that \( N_{p_i}(H \cap P_i) \) centralizes and hence normalizes \( H \cap P_j \) for all \( j \in \{1, 2, \ldots, n\} - \{i\} \).

This yields \( N_{p_i}(H \cap P_i) \leq N_G(H) \)

(c) \( \Rightarrow \) (d) If \( H \) is a maximal subgroup of \( G \), then \( H \not\leq N_G(H) \leq G \) gives that \( N_G(H) = G \).

(d) \( \Rightarrow \) (a) Let \( P \in \text{Syl}_p G \), and assume that \( N_G(P) \not\leq G \). Let \( M \) be a maximal subgroup of \( G \) containing \( N_G(P) \). Since \( M \not\leq G \) by assumption we get by Frobenius argument \( G = MN_G(P) \). But this yields the contradiction \( G = M \), as \( N_G(P) \leq M \).

Thus \( N_G(P) = G \) for any prime \( p \), and \( G \) is nilpotent.

(a) \( \Rightarrow \) (e) If \( G \) is nilpotent, and \( N \not\leq G \), then \( G/N \) is also nilpotent. So it suffices to show that \( Z(G) \neq \{e\} \), if \( G \) is a nilpotent group \( \{e\} \). If \( G \) is nilpotent, then \( G = P_1 \times P_2 \times \cdots \times P_n \) with \( P_i \in \text{Syl}_{p_i} G \). But then \( Z(G) = Z(P_1) \times Z(P_2) \times \cdots \times Z(P_n) \neq \{e\} \) by (2).

(e) \( \Rightarrow \) (a) By assumption \( Z(G) \neq \{e\} \) Thus \( |G/Z(G)| < |G| \) and \( G/Z(G) \) satisfies the condition (d). By induction on \( |G| \) we get that \( G/Z(G) \) is nilpotent. Then (3.12.9) gives that \( G \) is nilpotent.

(a) \( \Rightarrow \) (f) Let, \( y \in G, (\sigma(x), \sigma(y)) = 1 \). Since \( G \) is nilpotent, \( G = P_1 \times \cdots \times P_n \), \( P_i \in \text{Syl}_{p_i} G \). Then \( x = x_1x_2 \cdots x_n \), with \( x_i \in P_i, y = y_1 \cdots y_n, y_i \in P_i \).

Here \( x_i = e \), if \( p_i \) does not divide \( \sigma(x) \) and similarly \( y_i = e \) if \( p_i \) does not divide \( \sigma(y) \), \( i = 1, \ldots, n \). Since for \( i, j \in \{1, \ldots, n\} \) with \( i \neq j \) and \( g \in P_i, h \in P_j \) we have \( gh = hg \) we get \( xy = yx \).

(f) \( \Rightarrow \) (a) Let \( P \in \text{Syl}_p G \) and \( Q \in \text{Syl}_q G \), then for any \( x \in P \) and any \( y \in Q \) we have \( xy = yx \) the \( Q \leq N_G(P) \), if \( p \neq q \). This yields that \( G \leq N_G(P) \) and hence that \( G \) is nilpotent.
3.14. Proposition. Let $G$ be a group. If $N$ and $M$ are nilpotent, normal subgroups of $G$, then $NM$ is also a nilpotent, normal subgroup of $G$.

Proof. First we show that if $\{e\} \neq K \trianglelefteq H$ and $H$ is nilpotent, then $Z(H) \cap K \neq \{e\} : H$ is nilpotent, so $H = H_1 \times H_2 \times \cdots \times H_n$, $H_i \in Syl_{p_i} H$ and $Z(H) = Z(H_1) \times Z(H_2) \times \cdots \times Z(H_n)$. $K = K \cap H_i \in Syl_{p_i} K$ $i = 1, \cdots, n$, and $K$ is nilpotent by (3.12.b). Thus $K = K_1 \times K_2 \times \cdots \times K_n$ and there exists $i \in \{1, \cdots, n\}$ with $K_i \neq \{e\}$, since $K \neq \{e\}$. So by (2) we see that $\{e\} \neq K_i \cap Z(H_i) \leq K \cap Z(H)$.

If $N \cap M = \{e\}$, then $NM = N \times M$ and hence $NM$ nilpotent by (3.12.d). If $N \cap M = K \neq \{e\}$, then $\{e\} \neq K \cap Z(N) = Z(N) \cap M$ by the first paragraph as $K \leq N$ and $N$ is nilpotent. Since $N \leq G$ we get $Z(N) \leq G$ and hence $Z(N) \cap M \leq M$. So by the first paragraph $(Z(N) \cap M) \cap Z(M) = Z(N) \cap Z(M) \neq \{e\}$. Since $Z(N) \cap Z(M) \leq Z(NM)$ we get $S = Z(NM) \neq \{e\}$ and $Z(NM) \leq G$.

We have $NS/S \leq G/S$ and $MS/S \leq G/S$ and both $NS/S$ and $MS/S$ are nilpotent. By induction on $|G|$ we get that $(NS/S)(MS/S) = NMS/S = NM/S$ is nilpotent, normal in $G/S$. Since $NM/Z(NM)$ is nilpotent, we get that $NM$ is nilpotent by (3).

3.15. Definition. The product of all normal, nilpotent subgroups of a finite group $G$ is again a nilpotent normal subgroup of $G$ by (3). It is denoted by $F(G)$ and is called the Fitting subgroup of $G$. It is the normal subgroup of $G$ maximal subject to the condition of being nilpotent.

Exercises

1) a) Let $G$ be a finite group, $H \trianglelefteq G$, and let $p$ be a prime not dividing $[G : H]$. Then every Sylow $p$-subgroup of $G$ is contained in $H$.

   b) If $K \trianglelefteq G$ with $|K| = p^b$, then $K$ is contained in every Sylow $p$-subgroup of $G$.


2) If $G$ is a finite $p$-group of order $p^n$, then there exist $N_i < G$, $i = 0, \cdots, n$ with $N_0 = \{e\} < N_1 < N_2 < \cdots < N_{n-1} < N_n = G$, that is $|N_i| = p^i$ for $i = 0, \cdots, n$. 
3) a) If $|G| = pq$, $p, q$ primes with $p < q$. Then a Sylow $q$-subgroup of $G$ is normal in $G$. If furthermore $p$ does not divide $q - 1$, then $G$ is cyclic.
   b) If $|G| = p^2q$, $p, q$ primes, then $G$ contains a normal Sylow subgroup.
   c) If $|G| = 144$, then $G$ is not simple.

4) Let $P \in Syl_p G$ and let $\rho$ be the permutation representation of $G$ on the left cosets of $N_G(P)$. Prove
   a) $\rho(P)$ fixes exactly one point.
   b) If $|P| = p$, then $\rho(x)$ is a product of one 1-cycle and a certain number of $p$-cycles for any $x \in P - \{e\}$.
   c) If $|P| = p$ and $y \in N_G(P) - C_G(P)$, then $\rho(y)$ fixes at most $r$ cosets of $N_G(P)$, where $r$ denotes the number of orbits of $P$.
   d) Use the above results, to show that a group of order 264 is not simple.

5) Let the group $G$ act transitively on the set $X$. Let $K \trianglelefteq G$ and assume that $K$ also acts transitively on $X$. Then $G = K \cdot G_x$ for any $x \in X$. Deduce from the above result the Frattini argument.

6) Let $\rho$ be the regular representation of the finite group $G$. Show that $\rho(G)$ consists of even permutations only (that is, $\rho(G) \leq A_{|G|}$) if and only if the Sylow 2-subgroups of $G$ are not cyclic.

7) (Thompson Transfer Lemma) Let $G$ be a finite group of even order and let $T \in Syl_2 G$ and $S$ a maximal subgroup of $T$. If there exists an involution $t \in T$, that is, $t^2 = e \neq t$, such that $gtg^{-1} \notin S$ for every $g \in G$, then $G$ has a subgroup of index 2.
   (Hint: Consider the permutation representation $\rho$ of $G$ on the left cosets of $S$ and find $\text{sign}(\rho(t))$).

8) Give new proofs for the existence of Sylow subgroups in the following way:
   1) Let $G$ be a minimal counter example for $p, p$ a prime. Show:
      (a) If $H \not\subseteq G$, then $p$ does not divide $|G : H|$.
      (b) $G$ has no normal subgroups $N$ with $|N| = p^k$ for some $k \in \mathbb{N} - \{0\}$.
      (c) Using class equation, derive a contradiction from (a) and (b).
II) (a) Without using Sylow’s theorem, show that if $H \not\subseteq G$ and $P \in Syl_p G$, then there exists $g \in G$ with $gPg^{-1} \cap H \in Syl_p H$.

(b) Let $V$ be a vector space over the field $GF(p)$ with $p$ elements of dimension $|G|$ in a basis $B = \{v_x | x \in G\}$.

Let $T_g : V \rightarrow V$ be the linear operator on $V$ given on $B$ by $T_g(v_x) = v_{g,x}$, $x \in G$. Then $T : G \rightarrow GL(|G|, p)$ defined by $T(g) = T_g$ is a monomorphism.

(c) $GL(|G|, p)$ has Sylow $p$-subgroups. (See Exercise ? of Chapter I.)

(d) Deduce that $T(G)$ and hence $G$ has Sylow $p$-subgroups.

9) (a) If $P_1$ and $P_2$ are Sylow $p$-subgroups of the group $G$, and if $Z(P_1) \leq P_2$, then $Z(P_1) = Z(P_2)$.

(b) Let $P$ be a $p$-subgroup of the finite group $G$ such that $P \in Syl_p N_G(P)$. Then $P \in Syl_p G$.

(c) Let $H$ be a subgroup of $G$ containing $N_G(P)$ for some $P \in Syl_p S$. Then $|G : H| \equiv 1 (p)$.

(d) Let $G$ be a finite group and $\{P_1, P_2, \cdots, P_n\} = Syl_p G$. If $|P_i : P_i \cap P_j| \geq p^d$ for all $i, j \in \{1, \cdots, n\}$, $i \neq j$, then $n \equiv 1 \pmod{p^d}$.

(Hint: Consider the double coset representation of $G$ with respect to $(P_1, N_G(P_1))$ and use $n = [G : N_G(P_1)]$)

(e) Let $G$ be a finite group with abelian Sylow $p$-subgroups. If $\bigcap_{P \in Syl_p G} P = \{e\}$, then there exist $P_1, P_2 \in Syl_p G$ with $P_1 \cap P_2 = \{e\}$.

(Hint: Let $G$ be a minimal counter example with $|Syl_p G|$ as small as possible. For $P_i \in Syl_p G$, $i = 1, \cdots, k$, assume that $P_2 \cap P_3 \cap \cdots \cap P_k = A \neq \{e\}$ and $P_1 \cap A = \{e\}$. Consider $C_G(A)$).

10) The finite group $G$ is nilpotent if and only if $<x, y>$ is nilpotent for any $x, y \in G$.

11) Let $G$ be a finite nilpotent group with $P_i \in Syl_p G$, $i = 1, \cdots, r$. Then $\text{Aut} G \cong \text{Aut} P_1 \times \text{Aut} P_2 \times \cdots \times \text{Aut} P_r$.

12) Let $G$ be a finite group, $P \leq G$, $P$ a $p$-group, $A \leq G$ such that $PA = G$.

If $C_A(P) = \{a \in A | ax = xa \text{ for all } x \in P\} = \{e\}$, then $p$ does not divide $|A|$.
13) An element of order 2 of a group $G$ is called an **involution** of $G$.

(a) If $u$ and $v$ are two distinct involutions of the group $G$, then $<u, v>$ is isomorphic to a dihedral group.

(b) Let $u$ and $v$ be involutions of $G$. If $uv$ is of odd order, then $u$ is conjugate to $v$ in $G$ (actually they are conjugate to each other in $<u, v>$).

If $uv$ is of order $2n$, then $(uv)^n = w$ is also an involution and $u, v \in C_G(w)$.

(c) Suppose the group $G$ contains a subgroup $H$ of even order, which does not contain every involution in $G$. Suppose that for any involution $t \in H$ we have $C_G(t) \leq H$. Show that if $u \in H$ and $v \in G \setminus H$ are two involutions of $G$, then $u$ is conjugate to $v$ in $G$. Deduce that all involutions of $G$ are conjugate to each other in $G$.

(d) Suppose that the finite group $G$ contains exactly two conjugacy classes of involutions. Let $u_1$ and $u_2$ be non-conjugate involutions of $G$, and $K_i$ be the conjugacy classes of $G$ with $u_i \in K_i$, $i = 1, 2$. Let $S_i = \{(x, y) | x \in K_1, \, y \in K_2 \text{ and } (xy)^n = u_i \text{ for some } n \in \mathbb{N}\}$. Then $|G| = |C_G(u_1)| \cdot |S_2| + |C_G(u_2)| \cdot |S_1|$.

(Hint: $\frac{|G|}{|C_G(u_1)|} \cdot \frac{|G|}{|C_G(u_2)|} = |K_1 \times K_2|$. On the other hand for any $x \in K_1$ and $y \in K_2$, $o(xy) = 2n$ by (b) and (c) and $(xy)^n \in K_1$ or $K_2$, thus $|K_1 \times K_2| = \frac{|G|}{|C_G(u_1)|} \cdot |S_1| + \frac{|G|}{|C_G(u_2)|} \cdot |S_2|$).

14) An abstract characterization of $S_5$:

Let $G$ be a finite group containing exactly two conjugacy classes of involutions and let $u_1, u_2$ be representatives of these classes. Suppose that $C_G(u_1) \cong <u_1> \times S_3$ and $C_G(u_2) \cong D_8$. Then $G \cong S_5$.

(Hint: (a) $C_G(u_2)$ is a Sylow 2-subgroup of $G$. In particular we can assume that without loss of generality. $u_1 \in C_G(u_2)$.

(b) Using (13,d) compute $|G|$, $(|G| = 120)$ as follows:

i) $C_G(u_2)$ contains 3 conjugacy classes of involutions. If $x \in C_G(u_2) \setminus \{u_2\}$ with $x^2 = e$, then $x$ is conjugate to $xu_2$ in $C_G(u_2)$. Deduce that $|S_2| = 4$.

ii) $C_G(u_1)$ contains 3 conjugacy classes of involutions. If $x \in C_G(u_1) \setminus \{u_1\}$ with $x^2 = e$, then $x$ is not conjugate to $xu_1$ in $C_G(u_1)$. Hence exactly one of the involutions $x$ and $xu_1$ is conjugate to $u_1$. Deduce that $|S_1| = 9$. 

(c) There exists a four subgroup $V$ of $C_G(u_2)$, with $u_2 \in V$ such that all involutions of $V$ is conjugate to $u_2$ in $G$.

(d) $C_G(V) = V$ and $N_G(V)$ contains at least two Sylow 2-subgroups of $G$.

(e) $N_G(V)/C_G(V) = N_G(V)/V \cong \text{Aut}S_3 \cong S_3$ and hence $|N_G(V)| = 24$.

(f) $|G : N_G(v)| = 5$ and the permutation representation of $G$ on the set of all left cosets of $N_G(V)$ gives an isomorphism of $G$ onto $S_5$.

15) An abstract characterization of $A_5$:

Let $G$ be a finite simple group and $T \in \text{Syl}_2G$. Suppose that $|T| = 4$ and for all $x \in T - \{e\}$ we have $C_G(x) = T$. Then $G \cong A_5$.

(Hint: (a) $T$ is a four group and $N_G(T) \cong A_4$. (Use Exercise of Chapter II and Exercise 7 and (??)). $G$ contains exactly one conjugacy class of involution.

(b) Every coset of $T$ in $G - N_G(T)$ contains a unique involution. Every coset of $N_G(T)$ in $G$ contains exactly 3 involutions.

(c) Let $u \in N_G(T) - T$. Then $C_G(u) \leq N_G(T)$. Let $x \in C_G(u) - < u >$. Then $Tx \subseteq G - N_G(T)$. Let $v$ be the unique involution of $Tx$ by (b). So $x = tv$ for some $t \in T$ and $x^u = x = tv^u$ with $t^u \in T$. This gives $Tv^u = Tv$ and hence $v^u = v$ by (b). This contradicts the structure of the centralizer of an involution since $u$ is of odd order.

(d) Let $z_1, z_2, z_3$ be the involutions in $N_G(T)z_1 \neq N_G(T)$ and $y_1, y_2, y_3$ be the involutions in $N_G(T)y_1 \neq N_G(T)$. (see (b)). Assume that $N_G(T)y_1 \neq N_G(T)z_1$. Then $\{z_1z_2, z_1z_3\} \leq N_G(T) - T$, $\{y_1y_2, y_1y_3\} \leq N_G(T) - T$. Furthermore $\{z_1z_2, z_1z_3\} \cap \{y_1y_2, y_1y_3\} = \phi$, since otherwise $z_1z_2 = y_1y_2 = a \in N_G(T) - T$ and both $y_1$ and $z_1$ invert $a$, thus $y_1z_1$ centralizes $a$, by (c) this gives $N_G(T)y_1 = N_G(T)z_1$.

(e) Deduce from (d) that $|G : N_G(T)| = 5$. The permutation representation of $G$ on the left cosets of $N_G(T)$ gives then an isomorphism of $G$ onto $A_5$. 

CHAPTER IV

Elementary remarks about Solvable Groups:

4.1. Definition. Let $G$ be a group. For any $x, y \in G$, the element $x^{-1}y^{-1}xy$ is called the \textit{commutator} of $x$ and $y$ and is denoted by $(x, y) = x^{-1}y^{-1}xy$. The subgroup $\langle (x, y) | x \in G, y \in G \rangle$ generated by the commutators is called the commutator subgroup of $G$ and is denoted by $G'$. We define recursively $G^{(0)} = G, G^{(1)} = G'$ and $G^{(i+1)} = (G^{(i)})'$.

4.2. Theorem. (a) If $\alpha$ is any homomorphism of $G$ into some group, then $\alpha(G^{(i)}) = (\alpha(G))^{(i)}$ for any $i \in \mathbb{N}$. In particular $\alpha(G^{(i)}) = G^{(i)}$ for any automorphism $\alpha$ of $G$. If $N$ is a normal subgroup of $G$, then $N^{(i)} \triangleleft G$ for any $i \in \mathbb{N}$.

\begin{itemize}
  \item[(b)] $(G^{(i)})^{(j)} = G^{(i+j)}$, for any $i, j \in \mathbb{N}$.
  \item[(c)] If $N \triangleleft G$, then $(G/N)^{(i)} = G^{(i)}N/N$, for any $i \in \mathbb{N}$.
  \item[(d)] $G/G'$ is abelian. If $N \triangleleft G$ and $G/N$ is abelian, then $G' \leq N$.
\end{itemize}

Proof. (a) For any $x, y \in G$ we have $\alpha([x, y]) = \alpha(x^{-1}y^{-1}xy) = \alpha(x)^{-1}\alpha(y)^{-1}\alpha(x)\alpha(y) = [\alpha(x), \alpha(y)]$. Thus $\alpha(G') = \langle [\alpha(x), \alpha(y)] | x, y \in G \rangle = \alpha(G)'$. Induction on $(i)$ gives then the result.

If $\alpha$ is an automorphism, then $\alpha(G) = G$ and hence $\alpha(G^{(i)}) = \alpha(G)^{(i)} = G^{(i)}$.

If $N \triangleleft G$, then the map $\tau_g : N \to N$ defined by $\tau_g(x) = gxg^{-1}$ is an automorphism of $N$, for any $g \in G$. This yields the result.

(b) Follows by induction.

(c) Let $N \triangleleft G$, then for any $x, y \in G$ we have $[xN, yN] = [x, y]N$ and hence $(G/N)' = \langle [xN, yN] | x, y \in G \rangle = \langle [x, y]N | x, y \in G \rangle = G'/N/N$.

The assertion follows then by induction on $i \in \mathbb{N}$.

(d) For any $x, y \in G$ we have $[xG', yG'] = [x, y]G' = G'$, and hence $xG'$ and $yG'$ commute in $G/G'$ for any $x \in G$ and any $y \in G$. Thus $G/G'$ is abelian.

If $N \triangleleft G$ and $G/N$ is abelian, then $[xN, yN] = N$, that is, $[x, y] \in N$ for all $x, y \in G$. This yields $G' \leq N$.

4.3. Definition. A group $G$ is called \textit{solvable} if $G^{(k)} = \{e\}$, for some $k \in \mathbb{N}$. 
4.4. Theorem. (a) If $G$ is solvable, and $H \leq G$, then $H$ is solvable.

(b) If $G$ is solvable and $N \triangleleft G$, then $G/N$ is solvable.

(c) If $G_1$ and $G_2$ are solvable, then $G_1 \times G_2$ is solvable.

(d) If $N_1 \triangleleft G$, $N_2 \triangleleft G$ and $G/N_1$ and $G/N_2$ are solvable, then $G/N_1 \cap N_2$ is solvable.

(e) If $N \triangleleft G$ and both $N$ and $G/N$ are solvable, then $G$ is solvable.

(f) If $N_1 \triangleleft G$, $N_2 \triangleleft G$, and $N_1, N_2$ are solvable then $N_1 N_2$ is solvable.

(g) Every finite nilpotent group is solvable.

Proof. (a) Obviously $H' \leq G'$ and by induction $H^{(i)} \leq G^{(i)}$ for all $i$. Since there exists $k \in \mathbb{N}$ with $G^{(k)} = \{e\}$, we get that $H^{(k)} = \{e\}$ and hence that $H$ is solvable.

(b) $(G/N)^{(k)} = G^{(k)} N/N = N/N = \{N\}$ for some $k \in \mathbb{N}$.

(c) For any $g_1, h_1 \in G_1$ and $g_2, h_2 \in G_2$ we have $[g_1 g_2, h_1 h_2] = g_2^{-1} g_1^{-1} h_1^{-1} h_1 g_1 g_2 h_1 h_2 = g_2^{-1} h_2^{-1} (g_1^{-1} h_1^{-1} g_1 h_1) g_2 h_2 = [g_1, h_1][g_2, h_2]$ since for any $x \in G_1$, $y \in G_2$ we have $x y = y x$. Thus $(G_1 \times G_2)' = G_1' \times G_2'$ and by induction $(G_1 \times G_2)^{(i)} = G_1^{(i)} \times G_2^{(i)}$. This yields the assertion.

(d) Let us consider the map $\alpha : G \to (G/N_1) \times (G/N_2)$ defined by $\alpha(g) = (g N_1, g N_2)$. It is easy to see that $\alpha$ is a homomorphism with $\ker(\alpha) = \{g \in G \mid g N_1, g N_2\} = (N_1, N_2) = N_1 \cap N_2$. Thus $G/N_1 \cap N_2$ is isomorphic to a subgroup of $(G/N_1) \times (G/N_2)$. The assertion follows then from (c) and (a).

(e) If $N \triangleleft G$ with $G/N$ solvable, then there exists $k \in \mathbb{N}$ with $(G/N)^{(k)} = G^{(k)} N/N = \{N\}$, that is, $G^{(k)} \leq N$. If $N$ is also solvable, then $(G^{(k)})^{(\ell)} = \{e\}$ for some $\ell \in \mathbb{N}$ by (a). By (?) we get then $G^{(k+\ell)} = \{e\}$ and hence $G$ is solvable.

(f) $N_1 N_2 / N_1 \cong N_2 / N_1 \cap N_2$ is solvable by (b) since $N_2$ is solvable, and since $N_1$ is also solvable we get by (e) that $N_1 N_2$ is also solvable.

(g) Let $G$ be a nilpotent group, then $Z(G) \neq \{e\}$. $G/Z(G)$ is also nilpotent of order less than $|G|$. By induction $G/Z(G)$ is solvable, and hence by (e) $G$ is solvable, since $Z(G)' = \{e\}$. \hfill $\square$

4.5. Example.

1) $G = S_4$ is solvable with the following derived series:

Since $S_4 / A_4$ is of order two and hence abelian we have $G' \leq A_4$. Since $(12)(13)(12)(13) = (132)(132) = (123)$ we get that 3 divides $|G'|$. Since a Sylow 3-subgroup of $S_4$ is not normal in $G$, a Sylow 3-subgroup of $G'$ cannot be normal in $G'$. Thus $G'$ contains at least and hence exactly 4 Sylow 3-subgroups. Thus $12 \leq |G'|$ and hence $G' = A_4$. 

Let $V = \langle (12)(34), (13)(24) \rangle$. Then $V \leq A_4$ and $A_4/V$ is of order 3. Thus $G'' \leq V$. Since $G' = A_4$ is not abelian $|G''| \neq 1$. Since an element of order 3 acts transitively on the set of subgroups of $V$ of order 2, we get $G'' = V$ and $G^{(3)} = \{e\}$.

The maximal subgroups of $G$ are

1) the conjugates of Sylow 2-subgroups each of index 3
2) the conjugates of the normalizers of Sylow 3-subgroups each isomorphic to $S_3$ and of index 4.

2) $G = S_5$ is not solvable, $G' = A_5$, $G'' = G' \neq \{e\}$.

The maximal subgroups of $A_5$ are,

the conjugates of normalizers of Sylow 2-subgroups each isomorphic to $A_4$ and of index 5,
the conjugates of normalizers of Sylow 5-subgroups each of index 5,
the conjugates of normalizers of Sylow 3-subgroups each of index 10.

$A_5$ contains no subgroups of order 15,20.

4.6. Theorem. Let $G$ be a group of order $|G| = p^nq$, $p, q$ primes, then $G$ is solvable.

Proof. If $p = q$, then $G$ is a $p$-group and solvable by (?). So we can assume that $p \neq q$. Let $G$ be a minimal counter example to the theorem.

(a) $G$ is simple: If $\{e\} \neq N \not\leq G$, then both $N$ and $G/N$ have orders less than $|G|$ and hence these are not counterexamples to the theorem. So both $N$ and $G/N$ are solvable and hence $G$ is solvable by (?), contradicting the choice of $G$. So $G$ is simple.

(b) If $P_1, P_2 \in \text{Syl}_pG$ and $P_1 \neq P_2$, then $P_1 \cap P_2 = \{e\}$.

Let us choose $P_1, P_2 \in \text{Syl}_pG$, $P_1 \neq P_2$ such that $D = P_1 \cap P_2$ is of maximal possible order. Assume that $\{e\} \neq D$. Since $D \not\leq P_i$, we have $N_{P_i}(D) \not\geq D$, $i = 1, 2$. If $N_G(D)$ is a $p$-group, then there exists a Sylow $p$-subgroup $P_i$ of $G$ with $N_G(D) \leq P_i$. But then $D \not\leq N_{P_i}(D) \leq P_i \cap P_3$ $i = 1, 2, 3$ yields that $P_1 = P_3 = P_2$ by our choice of $D$. This is a contradiction. So $N_G(D)$ is not a $p$-group. Let $Q \in \text{Syl}_qN_G(D)$ and let $P \in \text{Syl}_pG$ with $N_{P_i}(D) \leq P$. Then $|PQ| = \frac{|P||Q|}{|P \cap Q|} = |P||Q| = |G|$ gives that $PQ = G$. Then for any $g \in G$ there exists $y \in Q$ and $x \in P$ such that $xy = g$. This gives $gDg^{-1} = xyDy^{-1}x^{-1} = xDx^{-1} \leq P$. 


and hence \( \{e\} \neq D \leq K = < qDg^{-1}g \in G > \leq P \subsetneq G \). Since \( K \triangleleft G \) we get a contradiction to \((a)\). So \( D = \{e\}\).

c) Let \( G = \bigcup_{i=1}^{q} g_iN_G(P) \), where \( N_G(P) = P, P \in \text{Syl}_qG \), be the decomposition of \( G \) into left cosets of \( N_G(P) \). Then the subset \( \bigcup_{i=1}^{q} g_iP^{-1}g_i - \{e\} \) contains \((|P|-1)q = |G| - q \) elements.

So the subset \( Q = G - \bigcup_{i=1}^{q} g_iP^{-1}g_i - \{e\} \) must be a Sylow \( q \)-subgroup of \( G \). Thus \( G \) contains a unique Sylow \( q \)-subgroup, which must be normal, contradicting \((a)\).

This last contradiction shows that there exists no counterexample to the theorem. \( \square \)

4.7. Theorem. (Ito) Assume that \( G = AB \) with abelian subgroups \( A \) and \( B \) of \( G \). Then \( G' = \{e\} \). In particular \( G \) is solvable.

Proof. Let \( [A, B] = < [a, b] | a \in A, b \in B > \). We show first that \( [A, B] = G' \). For any \( a_1, a_2 \in A \) and \( b \in B \) we have \( a_1^{-1}ba_1 = a_2b_2 \) for some \( a_2 \in A \) and \( b_2 \in B \), and

\[
\begin{align*}
(a_1b_1)^{-1}[a, b](a_1b_1) = b_1^{-1}[a_1^{-1}aa_1, a_1^{-1}ba_1]b_1 = b_1^{-1}[a, a_2b_2]b_1 = b_1^{-1}[a, b]b_1
\end{align*}
\]

Similarly for any \( a \in A \) and any \( b, b_1 \in B \) we have \( b_1^{-1}[a, b]b_1 = [a^*, b] \in [A, B] \) for some \( a^* \in A \). Thus \( [A, B] \leq AB = G \). As \( A \) and \( B \) are abelian we get that \( G/[A, B] \) is abelian. Thus \( G' \leq [A, B] \leq G' \), and hence \( [A, B] = G' \).

Next we show that \( G' \) is abelian. Let \( a, a_1 \in A, b, b_1 \in B \). Then \( a_1^{-1}ba_1 = a_2b^* \) for some \( a_2 \in A, b^* \in B \) and \( b_1^{-1}ab_1 = b_2a^* \in BA = AB = G \) for some \( b_2 \in B \) and \( a^* \in A \). We get

\[
(a_1b_1)^{-1}[a, b](a_1b_1) = b_1^{-1}[a_1^{-1}aa_1, a_1^{-1}ba_1]b_1 = b_1^{-1}[a, a_2b_2]b_1 = b_1^{-1}[a, b]b_1
\]

\[
= [b_1^{-1}ab_1, b_1^{-1}b^*b_1] = [b_2a^*, b^*] = [a^*, b^*]
\]

and

\[
(b_1a_1)^{-1}[a, b](b_1a_1) = a_1^{-1}[b_1^{-1}ab_1, b_1^{-1}ba_1]a_1 = a_1^{-1}[b_2a^*, b]a_1 = a_1^{-1}[a, b]a_1
\]

\[
= [a^*, a_2b^*] = [a^*, b^*].
\]

Thus \( [a, b][a_1b_1^{-1}b_1^{-1}] = a_1b_1a_1^{-1}b_1^{-1}[a, b] \), that is, \( [a, b][a_1^{-1}, b_1^{-1}] = [a_1^{-1}, b_1^{-1}][a, b] \)

implying that \( G' \) is abelian, since \( G' \) is generated by the commutators \( [a, b], a \in A, b \in B \). Thus \( G'' = \{e\} \). \( \square \)
4.8. **Corollary.** If $G$ is a group of order $p^2q^2$, $p, q$ primes, then $G$ is solvable.

**Proof.** Let $P \in \text{Syl}_pG$ and $Q \in \text{Syl}_qG$. If $p = q$, then $G$ is a $p$-group and hence $G$ is solvable. If $p \neq q$, then $G = PQ$, since $|PQ| = \frac{|P||Q|}{|P \cap Q|} = |P||Q| = p^2q^2 = |G|$. Thus $G = P \times Q$. Since any $p$-group of order at most $p^2$ is abelian, we get by (?!) that $G$ is solvable. 

4.9. **Theorem.** (O. Schmidt) Let $G$ be a finite group. If all proper subgroups of $G$ are nilpotent, then $G$ is solvable.

**Proof.** Let $G$ be a minimal counterexample to the theorem.

(a) $G$ is simple: Otherwise $G$ has a normal subgroup $N$ with $\{e\} \neq N \neq G$. Then $N$ is nilpotent and hence solvable. And every proper subgroup of $G/N$ is of the form $H/N$ for some subgroup $H$ of $G$ with $N \leq H \not\subset G$, and hence $G/N$ satisfies the hypothesis of the theorem. Since $|G/N| < |G|$, $G/N$ is not a counterexample to the theorem, so $G/N$ is solvable. Thus both $N$ and $G/N$ are solvable yielding that $G$ is solvable by (?!). This contradicts the choice of $G$ as a counterexample.

(b) By (a) $G$ has more than one maximal subgroups. Let $H_1, H_2$ be any two distinct maximal subgroups of $G$. Then $H_1 \cap H_2 = \{e\}$.

Let $H_1, H_2$ be two distinct maximal subgroups of $G$ chosen such that $D = H_1 \cap H_2$ is of maximal order. Assume that $D \neq \{e\}$. By (a) $N_G(D)$ is a proper subgroup of $G$. Let $H$ be a maximal subgroup of $G$ with $N_G(D) \leq H$. Then $D \not\subset N_H(D) \leq H$, by ( ) since $H$ are nilpotent and $D \not\subset H_i$, $i = 1, 2$. Thus $|H_i \cap H| \supseteq |H_1 \cap H_2|$. By our choice of $D$ this is possible only if $H = H_i$, $i = 1, 2$. But this is a contradiction. Thus $D = \{e\}$.

(c) Let $\mathcal{M}$ be the set of all maximal subgroups of $G$. Then $G$ acts on $\mathcal{M}$ by conjugation. Let $\mathcal{M}_i$, $i = 1, 2, \ldots, r$ be the orbits of $G$ on $\mathcal{M}$ and let $M_i \leq \mathcal{M}_i$, $i = 1, 2, \ldots, r$. By (a) and the maximality of $M_i$ we get $N_G(M_i) = M_i$ and hence $|\mathcal{M}_i| = |G : M_i|$, $i = 1, \ldots, r$. Since $G - \{e\} = \bigcup_{M \in \mathcal{M}} (M - \{e\})$ is a disjoint union by (b) we get

$$|G| - 1 = \sum_{M \in \mathcal{M}} ((|M| - 1) = \sum_{i=1}^r |G : M_i|(|M_i| - 1) = \sum_{i=1}^r |G| - \sum_{i=1}^r |G : M_i| = r|G| - \sum_{i=1}^r |G : M_i|$$

since $|G : M_i| \leq \frac{|G|}{i}$, $i = 1, \ldots, r$, we get $|G| - 1 \geq r|G| - r\frac{|G|}{2} = r\frac{|G|}{2}$ and hence $r = 1$. But this implies that $|G| - 1 = |G| - |G : M_1|$, that is, $G = M_1$ and hence $G = \{e\}$. This is a contradiction.
So there exists no counterexample to the theorem.

4.10. Theorem. Let $G$ be a finite solvable group. Then

(a) Every minimal normal subgroup $N$ of $G$ is an abelian $p$-group for some prime $p$ (depending on $N$).

(b) Every maximal subgroup of $G$ has index $p^k$ for some prime $p$ (depending on $M$).

Proof. Let $G$ be a finite solvable group and $N$ a minimal element with respect to inclusion of $\{K|\{e\} \neq K, K \subseteq G\}$. Since every subgroup of $G$ is solvable, $N$ is also solvable and hence $N' \subseteq N$. By (4.2) $N' \leq G$ and so $N' = \{e\}$ by the minimality of $N$. Let $p$ be a prime dividing $|N|$ and $P \in \text{Syl}_p N$. Since $N$ is abelian, $P \subseteq N$ and hence $\{P\} = \text{Syl}_p N$. For any $g \in G$, $gPg^{-1} \in \text{Syl}_p N$ and thus $gPg^{-1} = P$. By the minimality of $N$ we get $P = N$. This proves (a).

Let now $M$ be a maximal subgroup of $G$ and $N$ a minimal normal subgroup of $G$. If $N \leq M$, then $M/N$ is a maximal subgroup of the solvable group $G/N$ and hence by induction on the order of $G$ we deduce that $|G/N : M/N| = |G : M|$ is a prime power. So we can assume that $N \nleq M$. Then $NM$ is a subgroup of $G$ containing $M$ properly. Since $M$ is maximal we get $NM = G$. Thus $|G : M| = |N : N \cap M|$ divides $|N|$ and this proves (b) by the first paragraph.

4.11. Remark. The converse of the above theorem is not true. (See (?).10)). The group $GL(3,2)$ is simple of order 168 and the maximal subgroups of it have index 8 or 7. But we have the following partial result.

4.12. Theorem. Let $G$ be a finite group and assume that for every maximal subgroup $M$ the index $|G : M|$ is a prime or a square of a prime. Then $G$ is solvable.

Proof. We proceed by induction on $|G|$. Let $N$ be a minimal normal subgroup of $G$. If $G/N \neq \{N\}$, then any maximal subgroup of $G/N$ is of the form $M/N$ with a maximal subgroup $M$ of $G$. Since $|G/N : M/N| = |G : M|$ we see that $G/N$ satisfies the assumptions of the theorem. As $|G/N| < |G|$ we get by induction that $G/N$ is solvable. So we need only to show that $N$ is also solvable by (4.4.d).

Let $p$ be the largest prime dividing $|N|$ and let $P \in \text{Syl}_p N$. Then by the Frattini argument we obtain $G = NN_G(P)$. If $N_G(P) = G$, then $P \leq G$ and the minimality of $N$ yields that $P = N$. Thus $N$ is nilpotent and hence solvable in this case. So
Thus $N \subseteq G$. Let $M$ be a maximal subgroup of $G$ containing $N_G(P)$. This gives $G = NN_G(P) = NM$ and hence $q^a = |G : M| = |N : M \cap M|$ with a prime $q$ and $1 \leq a \leq 2$. Since $P \leq N \cap N_G(P) \leq N \cap M$ and $P \in \text{Syl}_p N$ we get that $p \neq q$ and hence $q < p$. Since $|N : N_N(P)| = |N : N_G(P) \cap N| \equiv 1 \pmod{p}$ and $|M \cap N : N_M \cap N| \equiv 1 \pmod{p}$ we get that $|N : N \cap M| = q^a \equiv 1 \pmod{p}$, since $N_M \cap N = N_G(P) \cap N$. Thus $p$ divides $q^a - 1$. Since $q < p$ this is possible only if $a = 2$ and $p | q - 1$. This yields $q = 2$, $p = 3$. But then the $|N : N \cap M| = 4$ and the permutation representation $\rho$ of $N$ on the set of cosets of $N \cap M$ in $N$ gives a homomorphism of $N$ into $S_4$ with $\text{Ker} \rho \leq N \cap M$. Since $S_4$ and hence every subgroup of it is solvable, we get that $(N/\text{Ker} \rho)' = N''/\text{Ker} \rho \leq N/\text{Ker} \rho$. Thus $N' \leq N$. Since $N' \leq G$ and $N$ is minimal normal in $G$ we get that $N' = \{e\}$ and hence $N$ is solvable.

Exercises to Chapter IV

1) Let $G$ be a group $H, K, L \leq G$, $N \leq G$. We define

$[H, K] = \langle [h, k] | h \in H, k \in K \rangle$

$[H, K, L] = [[[H, K], L], [x, y, z] = [[x, y], z]$ for $x, y, z \in G$.

$x^y = y^{-1}xy$, $x, y \in G$.

Prove the following:

a) $[xy, z] = [x, z]^y[y, z]$ and $[x, yz] = [x, z][x, y]^z$ and $[x, y]^{-1} = [y, x]$. 

b) $[H, K] = [K, H]$.

c) $[H, K] \leq < H, K >$.

d) $H \leq N_G(K)$ if and only if $[H, K] \leq K$.

e) Assume $H \leq K$, $H \leq G$. Then $K/M \leq Z(G/H)$ if and only if $[G, K] \leq H$.

f) If $\alpha \in \text{Aut} G$ then $\alpha([H, K]) = [\alpha(H), \alpha(K)]$.

g) Let $H, K, L$ be normal subgroups of $G$. Then $[HK, L] = [H, L][K, L]$.

h) $[x, y^{-1}, z]^y[y, z^{-1}, x]^z[z, x^{-1}, y]^x = e$.

i) If $[H, K, L] \leq N$ and $[K, L, H] \leq N$, then $[L, H, K] \leq N$.

2) a) Prove that a group of order $pq^r$ with primes $p, q, r$, is solvable.

b) Prove that a group of order $12p$ with a prime $p \neq 5$, is solvable.

c) Let $G$ be a group with $|G| \leq 200$, $|G| \neq 60, 120, 168, 180$. Then $G$ is solvable.

d) If $|G| = 120, 180$, then $G$ is not simple.
c) If $G$ is not solvable and $|G| = 180$, then $G = N_1 \times N_2$ with $N_1 \cong A_5$ and $N_2 \cong \mathbb{Z}_3$.

3) Let $F$ be a finite field with $q = p^n$ elements for a prime $p$. For $a \in F^* = F - \{0\}$, $b \in F$ and $\alpha \in \text{Aut } F$, define the map $T(a, b, \alpha) : F \to F$ by

$$T(a, b, \alpha)(x) = a \cdot \alpha(x) + b \quad \text{for any } x \in F.$$  

a) Show that $G = \{T(a, b, \alpha)| a \in F^*, b \in F, \alpha \in \text{Aut } F\}$ is a group.

b) Find $|G|$.

c) Show that $G$ is solvable.

d) Show that $G \cong S_4$ if $p^n = |F| = 4$.

4) Let $G$ be any group. Consider the diagonal subgroup $D$ of the direct product $G \times G$, that is, $D = \{(g, g)| g \in G\}$. Show that $G$ simple if and only if $D$ is a maximal subgroup of $G \times G$.

5) Let $G_1$ and $G_2$ be finite solvable groups and $M$ a maximal subgroup of $G = G_1 \times G_2$. Show that at least one of the following three conclusions holds:

$G_1 \leq M$, $G_2 \leq M$, $M \triangleleft G$. 
CHAPTER V

Characteristic Subgroups

5.1. Definition. Let $G$ be a group. A subgroup $H$ of $G$ is called a characteristic subgroup of $G$, denoted by $H \text{char} G$, if for every automorphism $\alpha$ of $G$ we have $\alpha(H) = H$. A group $G$ is called characteristically simple, if the only characteristic subgroups of $G$ are $\{e\}$ and $G$.

5.2. Examples and Notations.
1) The following subgroups of a (finite) group $G$ are characteristic.
   a) $Z(G) = C_G(G) = \text{center of } G$.
   $G^{(i)} = i$-th derived group of $G$
   b) $O_p(G) = \text{maximal normal } p \text{ subgroup of } G = \bigcap_{P \in \text{Syl}_p G} P$, $p$ a prime.
   $O'_p(G) = \text{maximal normal subgroup of } G \text{ of order prime to } p$.
   $O_2'(G)$ is denoted by $O(G) = \text{maximal normal subgroup of } G \text{ of odd order}$.
   c) $F(G) = \text{maximal normal nilpotent subgroup of } G = \text{Fitting subgroup of } G$.
   d) $S(G) = \text{maximal normal solvable subgroup of } G$.
   e) Any normal subgroup $N$ of $G$ with $(|N|, |G/N|) = 1$

2) If $G$ is cyclic, then any subgroup of $G$ is characteristic.

3) Let $G$ be a (finite) $p$-group, for some prime $p$. Then
   $\Omega_i(G) := \langle g \in G | g^{p^i} = e \rangle$ and $\omega_i(G) = \langle g^{p^i} | g \in G \rangle$
   are characteristic subgroups of $G$, for any $i \in \mathbb{N}$.
   $\Omega_1(Z(G))$ is a nontrivial, elementary abelian, characteristic subgroup of $G$.

5.3. Theorem. Let $G$ be a group. Then
   a) If $H \text{char } K$ and $K \text{char } G$, then $H \text{char } G$.
   b) If $H \text{char } K$ and $K \trianglelefteq G$, then $H \trianglelefteq G$. In particular any characteristic subgroup of $G$ in normal in $G$.
   c) If $H \text{char } G$ and $K/H \text{char } G/H$, then $K \text{char } G$.
   d) If $H \text{ char } G$, then $C_G(H)$ and $N_G(H)$ are characteristic in $G$. 
Proof. Exercise.

5.4. Theorem. a) Let $G$ be a finite characteristically simple group. Then there exist normal subgroups $N_i$, $i = 1, 2, \ldots, r$, such that $N_1 \trianglelefteq N_2 \trianglelefteq \cdots \trianglelefteq N_r$, $N_1$ is a simple group, and $G = N_1 \times N_2 \times \cdots \times N_r$.

b) Let $G = N_1 \times N_2 \times \cdots \times N_r$ with simple nonabelian, isomorphic normal subgroups $N_i, i \in I = \{1, 2, \ldots, r\}$, then the only normal subgroups of $G$ are the subgroups $N_{i_1} \times N_{i_2} \times \cdots \times N_{i_s}$ for subsets $\{i_1, i_2, \ldots, i_s\} \subseteq I$. In particular the minimal normal subgroups of $G$ are $N_i, i \in I$.

c) Any (finite) direct product of isomorphic simple groups is characteristically simple.

d) The minimal normal subgroups of a group $G$ are characteristically simple. In particular if $G$ is a finite group and $N$ is a minimal normal subgroup of $G$, then either $N$ is an elementary abelian $p$-subgroup for some prime $p$ (which is the only possibility for solvable groups) or is the direct product of some isomorphic nonabelian simple groups.

Proof. a) Let $N$ be a minimal normal subgroup of $G$, and let $\mathcal{N} = \{\alpha(N) \mid \alpha \in \text{Aut}G\}$. Let $M$ be a subgroup of $G$, chosen to be maximal subject to the condition of being a direct product of some subgroups from $\mathcal{N}$. Assume that $\alpha(N) \not\trianglelefteq M$ for some $\alpha \in \text{Aut}G$. Since $\alpha(N)$ is also a minimal normal subgroup of $G$ and $M \trianglelefteq G$, we get $\alpha(N) \cap M = \{e\}$. Then we have by 5.1 that $\langle M, \alpha(N) \rangle = M \times \alpha(N)$ contradicting maximality of $M$. Thus we get that $\alpha(N) \leq M$ for all $\alpha \in \text{Aut}G$. But then $M = \langle \alpha(N) \mid \alpha \in \text{Aut}G \rangle$ is a characteristic subgroup of $G$ different from $\{e\}$.

Thus $M = G$ and $G = N_1 \times N_2 \times \cdots \times N_r$ with suitable $N_i = \alpha_i(N)$, $\alpha_i \in \text{Aut}G$, $i = 1, \ldots, r$. Since any normal subgroup of $N_i$ is a normal subgroup of $G$ and $N_i$ is a minimal normal subgroup of $G$, $N_i$ must be simple, $i = 1, 2, \ldots, r$. This proves (a).

b) Let $N \trianglelefteq G = N_1 \times \cdots \times N_r$, and $e \neq n = n_1n_2 \cdots n_r \in N$ with $n_i \in N_i$.

Then $N_j \leq N$ which will imply (b). Since $Z(N_j) = \{e\}$, there exists $x \in N_j$ with $[x, n_j] = c \neq e$. But since $N_j$ commutes elementwise with $N_i$, $i = 1, 2, \ldots, r$ but $j$ we get $[x, n_j] = [x, n] = c$. But then $e \neq c = [x, n] \in N \cap N_j$. Since $N_j$ is simple and $N \cap N_j \leq N_j$ we get $N_j \leq N$. 
c) Let $G = N_1 \times N_2 \times \cdots \times N_r$ with isomorphic simple groups $N_i$, $i = 1, 2, \cdots, r$. Assume first $N_1$ is not abelian. Then any nontrivial normal subgroup of $G$ contains at least one of the $N_i$, by (b). Let $\alpha$ be a permutation of $\{1, 2, \cdots, r\}$. Then the map $\tau_\alpha : G \to G$ with $\tau_\alpha(g_1, g_2, \cdots, g_r) = (g_{\alpha(1)}, g_{\alpha(2)}, \cdots, g_{\alpha(r)})$ is an automorphism of $G$ with $\tau_\alpha(N_i) = N_{\alpha(i)}$. Thus $\{e\}$ and $G$ are the only characteristic subgroups of $G$. Assume next that $N_i = \langle n_i \rangle$ is cyclic of order $p$ for some prime $p$, $i = 1, 2, \cdots, r$. Then the map $\mu : G \to V$ defined by $\mu(n_{a_1}, n_{a_2}, \cdots, n_{a_r}) = (a_1, a_2, \cdots, a_r)$ with $a_i \in F_p$, (the field with $p$ elements) is an isomorphism of $G$ onto the additive group of the vector space $V$ of dimension $r$ over the field $F_p$. The automorphisms of $V$ are the invertible, additive and hence linear (over $F_p$) transformations of $V$. If $v_1$ and $v_2$ are any two nonzero vectors of $V$, then there is a linear operator on $V$ which maps $v_1$ to $v_2$. Thus $AutG$ acts on $G - \{e\}$ transitively, in particular $G$ is characteristically simple.

d) follows from (a). \hfill \Box

5.5. Remark. ($\mathbb{Q}, +$) is characteristically simple. Thus the condition of finiteness in (5.4) is necessary.

5.6. Definition. Let $G$ be a group. We set $M = \{M | M$ is a maximal subgroup of $G\}$

$$\Phi(G) = \bigcap_{M \in M} M$$

the intersection of all maximal subgroups of $G$, is a characteristic subgroup of $G$, since any automorphism of $G$ induces a permutation on $M$ and is called the Frattini subgroup of $G$. By set theoretical conventions we have $\Phi(G) = G$ if $M = \phi$, that is, $G$ has no maximal subgroups. For finite groups, $\Phi(G) = G$ if and only if $G = \{e\}$.

In the following theorems we consider groups with maximal subgroups (or $G = \{e\}$).

5.7. Theorem. Let $G$ be a group. Then the following are equivalent:

a) $x \in \Phi(G)$

b) If $A$ is a subset of $G$ with $\langle x, A \rangle = G$, then $\langle A \rangle = G$.

Proof. (a) $\Rightarrow$ (b): If $\langle A \rangle \not\subseteq G$, then there exists a maximal subgroup $M$ of $G$ with $\langle A \rangle \leq M \not\subseteq G$. But then $\langle A, x \rangle = M \not\subseteq G$ since $x \in \Phi(G) \not\subseteq M$. So $\langle A \rangle = G$. 

(b) \( \Rightarrow \) (a): If there exists a maximal subgroup \( M \) with \( x \not\in M \), then \( \langle M, x \rangle = G \), but \( \langle M \rangle = M \neq G \). So \( x \in M \) for all maximal subgroups \( M \) of \( G \), that is, \( x \in \Phi(G) \).

5.8. Theorem. Let \( G \) be a group, \( N \trianglelefteq G \) and \( H \leq G \). Then
(a) If \( N \leq \Phi(H) \), then \( N \leq \Phi(G) \).
(b) \( \Phi(N) \leq \Phi(G) \).
(c) \( \Phi(H) \) is not necessarily a subgroup of \( \Phi(G) \).

Proof. If \( N \not\leq \Phi(G) \), then there exists a maximal subgroup \( M \) of \( G \) with \( N \not\leq M \). Then \( NM \) is a subgroup of \( G \) containing \( M \) properly, that is, \( G = NM \). Thus \( H = H \cap G = H \cap NM = N(H \cap M) = \Phi(H \cap M) = H \cap M \) by (5.7). Thus gives \( H \leq M \) and hence \( N \leq M \), since \( N \leq \Phi(H) \leq H \). But this is a contradiction. So \( N \leq \Phi(G) \).

(b) \( \Phi(N) \text{char} N \trianglelefteq G \) implies that \( \Phi(N) \leq G \). Apply (a) (by setting \( H := N \) and \( N := \Phi(N) \)).

(c) We have \( \Phi(S_4) = \{e\} \) and \( \Phi((1234)) = \langle(13)(24)\rangle \). \( \square \)

5.9. Theorem. (Gaschütz) Let \( M \) and \( N \) be normal subgroups of the finite group \( G \) such that \( N \leq M \cap \Phi(G) \). If \( M/N \) is nilpotent, then \( M \) is nilpotent.

Proof. Let \( P \in Syl_p M \). Then \( NP/N \in Syl_p M/N \) and hence \( NP/N \leq M/N \) as \( M/N \) is nilpotent. Since \( NP/N \text{char} M/N \leq G/N \) we get \( NP/N \leq G/N \) and hence \( NP \leq G \). Since \( P \in Syl_p M \) and \( NP \leq M \) we have \( P \in Syl_p NP \). By Frattini argument we get \( G = NP N_G(P) = NN_G(P) = \Phi(G) N_G(P) = N_G(P) \) by (5.7), since \( N \leq \Phi(G) \). Thus \( P \leq G \) and in particular \( P \leq M \). So \( M \) is nilpotent. \( \square \)

5.10. Theorem. Let \( G \) be a finite group. Then
a) (Frattini) \( \Phi(G) \) is nilpotent.
b) If \( G/\Phi(G) \) is nilpotent, then \( G \) is nilpotent.
c) (Wielandt) \( G \) is nilpotent if and only if \( G' \leq \Phi(G) \).
d) (Gaschütz) \( G' \cap Z(G) \leq \Phi(G) \).

Proof. a) Follows from (5.9) by letting \( N = M = \Phi(G) \).
b) Follows from (5.9) by letting \( N = \Phi(G) \) and \( M = G \).
c) Assume first that $G' \leq \Phi(G)$. Then $G/\Phi(G)$ is abelian and (b) implies that $G$ is nilpotent. Assume conversely that $G$ is nilpotent. Then any maximal subgroup $M$ of $G$ is normal in $G$ with $|G : M| = p$ for some prime $p$.

So $G/M$ is cyclic, in particular, abelian. Thus $G' \leq M$ for any maximal subgroup $M$ of $G$, that is, $G' \leq \Phi(G)$.

d) Let $D = G' \cap Z(G)$. If there exists a maximal subgroup $M$ of $G$ with $D \nsubseteq M$ then $DM = G$. Since $D \leq Z(G) \leq N_G(M)$ we get $M \leq G$ and hence $G/M$ is abelian. This gives $D \leq G' \leq M$. Therefore $D$ must be contained in each maximal subgroup of $G$, that is, $D = \Phi(G)$.

5.11. Theorem If $G$ is a finite $p$-group we have $\Phi(G) = < x^p, [x, y] | x, y \in G >$. In particular

a) $G/\Phi(G)$ is an elementary abelian group.

b) If $K \trianglelefteq G$ and $G/K$ is elementary abelian, then $\Phi(G) \leq K$.

Proof. Since $G$ is nilpotent we have $G' \leq \Phi(G)$ by (5.10.c). Let $M$ be a maximal subgroup of $G$, then $M \leq G$ and $|G/M| = p$. Thus $(Mx)^p = Mx^p = M$, that is, $x^p \in M$ for any $x \in G$. Thus $x^p \in \Phi(G)$ for all $x \in G$.

Let $D = < x^p, [x, y] | x, y \in G >$. We have shown that $D \leq \Phi(G)$. Since $G' \leq D$ we get $D \leq G$. Since $x^p \in D$ for any $x \in D$ the factor group $G/D$ is elementary abelian (of exponent $p$). So as in the proof of (5.4) we can consider $G/D$ as a vector space over the field $F_p$ with $p$ elements. Then every subgroup (subspace) of $G/D$ has a complementary subgroup (subspace). In particular $G/D = \Phi(G)/D \times H/D$ for some subgroup $H$ of $G$. But then $\Phi(G)H = G$ and hence $G = H$ by (5.7). This gives $1 = |G : H| = |G/D : H/D| = |\Phi(G)/D|$ and hence $D = \Phi(G)$. □