1. SL₂(ℤ)

Consider \( S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \), \( T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \) ∈ SL₂(ℤ). Note that we have

\[
S\left( \begin{array}{cc} a & b \\ c & d \end{array} \right) = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}, \quad T^m\left( \begin{array}{cc} a & b \\ c & d \end{array} \right) = \begin{pmatrix} a + mc & b + md \\ c & d \end{pmatrix}
\]

**Theorem 1.1.** SL₂(ℤ) = \( \langle S, T \rangle \).

*Proof.* Let \( A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \) ∈ SL₂(ℤ). We use induction on |c|.

Suppose first that \( c = 0 \). We have \( A = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = T^m \) or \( A = \begin{pmatrix} -1 & m \\ 0 & -1 \end{pmatrix} = (-I)T^{-m} = S^2T^{-m} \). In either case, we have \( A ∈ \langle S, T \rangle \).

Now we assume \( c ≠ 0 \). There is an integer \( n ∈ ℤ \) such that \( |a + nc| < |c| \) by division algorithm. We have

\[
ST^n\left( \begin{array}{cc} a & b \\ c & d \end{array} \right) = S\left( \begin{array}{cc} a + nc & b + nt \\ c & d \end{array} \right) = \begin{pmatrix} -c & -d \\ a + nc & b + nd \end{pmatrix} ∈ \langle S, T \rangle
\]

by induction hypothesis. Thus, \( A ∈ \langle S, T \rangle \).
2. The dihedral group $D_n$

**Definition 2.1.** A map $\phi : \mathbb{R}^2 \to \mathbb{R}^2$ is called a rigid motion if $\phi$ preserves the distance. $(d(\phi(a), \phi(b)) = d(a, b)$ for the usual distant function $d$ on $\mathbb{R}^2$).

**Example 2.2.** Rotations, translations, and reflections are examples of rigid motions.

**Definition 2.3.** Let $n \geq 3$ be an integer. Let $\Delta_n \subset \mathbb{R}^2$ be the regular $n$–gon centered at the origin with one vertice at $(1, 0)$. The dihedral group $D_n$ is defined as the group of rigid motions $\phi$ satisfying $\phi(\Delta) = \Delta$.

**Note 2.4.** Let $g \in D_n$.

1. $g$ maps the center to the center. (Otherwise, we have $\max_{a \in \Delta} d(g(0), a) > \max_{a \in \Delta} d(0, a)$, which is not possible)
2. $g$ maps vertices to vertices. (Vertices are characterized by the points in $\Delta_n$ with maximal distance from the center)
3. $g$ maps adjacent vertices to adjacent vertices.
4. If $A, B$ are adjacent vertices in $\Delta_n$, then $g$ is completely determined by $g(A)$ and $g(B)$.

**Theorem 2.5.** $|D_n| = 2n$.

**Proof.** Step 1 : $|D_n| \leq 2n$

Any $g \in D_n$ is completely determined by $g(A)$ and $g(B)$ for an adjacent pair of vertices $A, B$. We have at most $n$ choices for $g(A)$ from above, and have at most 2 choices for $g(B)$ corresponding to each choice of $g(A)$.

Step 2 : $|D_n| \geq 2n$

1. rotations
Let $r \in D_n$ be the counterclockwise rotation around the origin by $\frac{2\pi}{n}$. Then, $\{1, r, r^2, \ldots, r^{n−1}\}$ are all different elements in $D_n$ because they map $(1, 0)$ to different points.

2. reflections
There are reflections across the lines $y = \tan(\frac{k\pi}{n})x$ for each $k = 0, 1, \ldots, n − 1$. They are all different because they fix different set of points.

3. $\{\text{rotations}\} \cap \{\text{reflections}\} = \emptyset$

Since rotations fix all the points or none, and reflections fix two points, the intersection is empty.

By Step 1 and Step 2, we have $D_n = \{n \text{ rotations}\} \cup \{n \text{ reflections}\}$. \qed

**Theorem 2.6.** Let $s \in D_n$ be the reflection across the x–axis. Then,

$$D_n = \{1, r, r^2, \ldots, r^{n−1}, s, rs, r^2s, \ldots, r^{n−1}s\}$$

**Proof.** Note that $s, rs, \ldots, r^{n−1}s$ are all different elements in $D_n$. Also we have $\{1, r, \ldots, r^{n−1}\} \cap \{s, rs, \ldots, r^{n−1}s\} = \emptyset$ because $r^i = r^j s$ for some $i, j$ would imply $s = r^{i−j}$, but $s$ is not a rotation. By the previous theorem, $s, rs, \ldots, r^{n−1}s$ are all the reflections in $D_n$, and $D_n = \{1, r, \ldots, r^{n−1}, s, sr, \ldots, r^{n−1}s\}$. \qed

Consider the group operation on $D_n$. $r$ has order $n$, and any reflection has order 2 in $D_n$. $(rs)^2 = 1$ gives $srs = r^{−1}$ and $sr = r^{−1}s$. In general, we have $r^i(r^j s) = (r^j s)r^i$.

**Theorem 2.7.** Let $D_n$ be the dihedral group of order $2n$.

1. $[D_n, D_n] = \langle r^2 \rangle$.
2. $Z(D_n) = \begin{cases} 1 & \text{if } n \text{ is odd} \\ \{1, r^n \} & \text{if } n \text{ is even} \end{cases}$
3. A semi-direct product of two groups

**Definition 3.1.** Let $G, H$ be groups and $\phi : G \rightarrow Aut(H)$ be a group homomorphism. We define the semi-direct product of $G$ and $H$ with respect to $\phi$ by $H \rtimes_{\phi} G = (H \times G, \cdot)$ with
\[
(h, g) \cdot (h', g') := (h\phi(g)(h'), gg')
\]

**Example 3.2.** If $\phi$ is trivial (i.e., $\phi(g) = id_H$ for all $g \in G$), then $H \rtimes_{\phi} G \cong H \times G$.

**Example 3.3.** Consider $\phi : \mathbb{Z}/2\mathbb{Z} \rightarrow Aut(\mathbb{Z}/n\mathbb{Z})$ defined by $\phi(0) = id_{\mathbb{Z}/n\mathbb{Z}}$ and $\phi(1) = inv_{\mathbb{Z}/n\mathbb{Z}}$ where $inv_{\mathbb{Z}/n\mathbb{Z}}(a) = -a$. (Note that $inv_{\mathbb{Z}/n\mathbb{Z}} \in Aut(\mathbb{Z}/n\mathbb{Z})$ because $\mathbb{Z}/n\mathbb{Z}$ is abelian.) We have an isomorphism of groups $\Psi : D_n \rightarrow (\mathbb{Z}/n\mathbb{Z}) \rtimes_{\phi} (\mathbb{Z}/2\mathbb{Z})$ defined by $\Psi(r) = (1, 0)$ and $\Psi(s) = (0, 1)$. Note that $(0, 1)(1, 0) = (0 + \phi(1)(1), 1 + 0) = (-1, 1) = (-1, 0))(0, 1)$ corresponds to $sr = r^{-1}s$.

**Proposition 3.4.** $H \times \{1_G\} \leq H \rtimes_{\phi} G$, $\{1_H\} \times G \leq H \rtimes_{\phi} G$.

**Remark 3.5.** Suppose that $Q_8 = \{\pm 1, \pm i, \pm j, \pm k \mid i^2 = j^2 = k^2 = -1, ij = k\}$ is isomorphic to a direct product of two nontrivial groups $G, H$. Then we have two nontrivial subgroups $H \times \{1_G\}, \{1_H\} \times G$ which have a trivial intersection $\{1_H\} \times \{1_G\}$. This contradicts the fact that every nontrivial subgroup of $Q_8$ contains $\{\pm 1\}$. Thus, $Q_8$ is not a semi-direct product of two nontrivial groups.

4. Subgroups of $A_4$

$A_4 = \{1, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$

By Lagrange’s theorem, a subgroup of $A_4$ has order dividing 12. We can easily see that \langle (12)(34), (13)(24), (14)(23) \rangle are all subgroups of order 2, and \langle (123), (124), (134), (234) \rangle are all subgroups of order 3. $V_4 = \{1, (12)(34), (13)(24), (14)(23)\}$ is the only subgroup of order 4 because all the elements outside $V_4$ have order 3. We also have the trivial subgroup of order 1, and $A_4$ itself is a subgroup of order 12.

**Proposition 4.1.** $A_4$ does not have a subgroup of order 6.

**Proof.** Suppose $H$ is a subgroup of order 6. For any 3-cycle $(ijk) \in A_4$, $(ijk)^3 = 1 \in H$. Also $(ijk)^2 \in H$ since $(A_4 : H) = 2$. Thus $(ijk) \in H$, but there are eight of them. Contradiction! See also ([II]). \hfill \Box

**Proposition 4.2.** $\{1\}, V_4, A_4$ are the only normal subgroups of $A_4$.

**Proof.** Let $a, b \in A_4$ be elements of order 2, 3. Without loss of generality, we can write $a = (ij)(kl), b = (ijk)$ for $\{i, j, k, l\} = \{1, 2, 3, 4\}$. Note that
\[
(ijk)((ij)(kl))(ijk)^{-1} = (il)(jk)
\]
\[
((ij)(kl))(ijk)((ij)(kl))^{-1} = (ilj)
\]
This shows that no subgroup of order 2 or 3 is normal, and $V_4$ is normal in $A_4$. \hfill \Box

5. Frattini’s argument

**Theorem 5.1.** Let $G$ be a finite group with a normal subgroup $H$, and let $P$ be a Sylow $p$-subgroup of $H$. Then $G = N_G(P)H$. 

3
Proof. Recall $N_G(P) = \{g \in G \mid gp^{-1} = P\}$. Since $H$ is normal, for any $g \in G$, $g^{-1}Pg \subseteq g^{-1}Hg = H$. $g^{-1}Pg$ is also a Sylow $p$-subgroup of $H$, thus it is conjugate to $P$ in $H$. We have some $h \in H$ such that $g^{-1}Pg = h^{-1}Ph$, thus $gh^{-1} \in N_G(P)$, which implies $g \in N_G(P)H$. □

6. Determining Simplicity of Finite Groups

**Theorem 6.1.** (Useful counting result) Let $G$ be a finite group and $H$ be a subgroup of $G$. If $|G| \nmid (G : H)!$, then $G$ is not simple.

Proof. Let $\Sigma(G/H)$ be the permutation group of the left cosets of $H$. Define a group homomorphism $\lambda : G \to \Sigma(G/H)$ by $\lambda(g)(xH) = gxH$. Note that $\ker \lambda = \bigcap_{g \in G} gHg^{-1} \subseteq H$. If $\ker \lambda$ is trivial, then $|G| = |G/\ker \lambda| = |\im \lambda| \cdot |\Sigma(G/H)| = (G : H)!$. In other words, if $|G| \nmid (G : H)!$, then $\ker \lambda$ is a nontrivial normal subgroup of $G$, i.e., $G$ is not simple. □

Let $G$ be a finite group, and $n_p$ be the number of Sylow $p$-subgroups of $G$. The following are applications of Sylow theorems.

**Example 6.2.** Suppose $|G| = 200 = 2^3 \cdot 5^2$. Since $n_5 \equiv 1(5)$ and $n_5 \mid 8$, $n_5 = 1$ and the unique Sylow 5-subgroup is normal in $G$. Thus $G$ is not simple.

**Example 6.3.** Suppose $|G| = 495 = 3^2 \cdot 5 \cdot 11$. Assume that $G$ is simple. Since $n_3 \neq 1, n_5 \neq 1, n_{11} \neq 1$, we get $n_3 = 55, n_5 = 11, n_{11} = 45$. Thus there are 450 elements of order 11 and 44 elements of order 5. These elements and the identity are all the elements in $G$ by counting the number of elements, but $G$ must have an element of order 3. Contradiction! So $G$ is not simple.

**Example 6.4.** Suppose $|G| = 392 = 2^3 \cdot 7^2$. Consider a Sylow 7-subgroup $P_7$ of $G$. Since $7^2 \nmid |G| \nmid (G : P_7)! = 8!$, $G$ is not simple by the useful counting result.

**Example 6.5.** Suppose $|G| = 400 = 2^4 \cdot 5^2$. Assume that $G$ is simple and consider distinct Sylow 5-groups $P_1, P_2 \in Syl_5(G)$.

$$2^4 \cdot 5^2 = |G| \geq |P_1P_2| = \frac{|P_1||P_2|}{|P_1 \cap P_2|} = \frac{5^4}{|P_1 \cap P_2|}$$

shows that $|P_1 \cap P_2| = 5$. Note that $P_1, P_2$ are abelian because they have a prime square order. We have $P_1 \cap P_2 \leq P_1, P_2$ and $P_1P_2 \leq N_G(P_1 \cap P_2)$. $125 = |P_1|P_2| \leq |N_G(P_1 \cap P_2)| = 400$ gives $|N_G(P_1 \cap P_2)| = 200$ or 400. If $|N_G(P_1 \cap P_2)| = 200$, then it has index 2 in $G$, thus is normal in $G$. If $|N_G(P_1 \cap P_2)| = 400$, then $N_G(P_1 \cap P_2) = G$ and $P_1 \cap P_2$ is normal in $G$. In both cases, $G$ is not simple.

7. Classes of Finite Groups

**Definition 7.1.** Let $G$ be a group. Define the commutator subgroup $G^{(1)} = G' = [G, G] = \langle\{xyx^{-1}y^{-1} \mid x, y \in G\}\rangle$ and the $n$-th derived subgroup $G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$. We also define the center $Z(G) = \{x \in G \mid xg = gx \text{ for all } g \in G\}$ and $Z_n(G)$ by $Z(G/Z_{n-1}G) = Z_n(G)/Z_{n-1}(G)$. We have the following normal series of subgroups of $G$.

$$G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \cdots \geq G^{(n)} \geq \cdots$$

: derived series

$$\{e\} \leq Z_1(G) \leq Z_2(G) \leq \cdots \leq Z_n(G) \leq \cdots$$

: ascending central series

4
Theorem 7.2. Let $G$ be a finite group. $G$ is called nilpotent if $G$ satisfies one of the following equivalent conditions.

1. $Z_n(G) = G$ for some $n$.
2. If $H$ is a proper subgroup, then $H \leq N_G(H)$.
3. All Sylow subgroups of $G$ are normal.
4. $G$ is the direct product of its Sylow subgroups.

Proof. (1) $\Rightarrow$ (2) Since $H$ is proper, we have $Z_i(G) \leq H \leq Z_{i+1}(G)$ for some $i$. Note that $Z_i(G) \leq H$ and $H/Z_i(G) \leq Z_{i+1}(G)/Z_i(G)$ since $Z_{i+1}(G)/Z_i(G)$ is abelian. Thus $H \leq Z_{i+1}(G)$ and $H \leq Z_{i+1}(G) \leq N_G(H)$.

(2) $\Rightarrow$ (3) Let $P \in Syl_p(G)$. If $N_G(P) \not\leq G$, then by (2), $N_G(P) \leq N_G(N_G(P)) = N_G(P)$. Thus $N_G(P) = G$ and $P \leq G$.

(3) $\Rightarrow$ (4) Let $\{P_i\} = Syl_p(G)$ for each $p_i | |G|, i = 1, 2, \cdots, n$. Then $G = P_1P_2\cdots P_n \cong P_1 \times P_2 \times \cdots \times P_n$.

(4) $\Rightarrow$ (1) Let $G = P_1 \times P_2 \times \cdots \times P_n$ for $p_i$-group $P_i$. We know that $Z_1(P_i)$ is nontrivial. Since $P_i/Z_1(P_i)$ is also a $p_i$-group, $Z_2(P_i)/Z_1(P_i) = Z(P_i/Z_1(P_i))$ is nontrivial too. The ascending central series of $P_i$ is strictly increasing for all $i$, so we can find $N$ such that $Z_N(P_i) = P_i$ for all $i$. Thus $Z_N(G) = Z_N(P_1) \times \cdots \times Z_N(P_n) = G$ (Use induction for this). \qed

Theorem 7.3. Let $G$ be a finite group. $G$ is called solvable if $G$ satisfies one of the following equivalent conditions.

1. $G^{(n)} = \{e\}$ for some $n$.
2. $G$ has an abelian series (subnormal series with abelian quotient).
3. If $|G| = mn$ and $(m, n) = 1$, then $G$ has a subgroup of order $m$.

Proof. See ([H] pp.104-106). \qed

Example 7.4. If $G$ is abelian, then $G$ is solvable ($G^{(1)} = \{e\}$) and nilpotent ($Z_1(G) = G$). The derived series of $A_5$ never diminishes ($A_5^{(5)} = A_5$ for all $n$), and the ascending central series of $D_3$ never grows ($Z_n(D_3) = \{e\}$ for all $n$).

Definition 7.5. Let $G$ be a finite group. $G$ is called Lagrangian if $G$ has a subgroup of order $d$ for all $d | |G|$.

Now we consider the following classes of finite groups.

1. Cyclic $\subseteq$ (2) Abelian $\subseteq$ (3) Nilpotent $\subseteq$ (4) Lagrangian $\subseteq$ (5) Solvable $\subseteq$ (6) All finite groups

(1) $\Rightarrow$ (2) Clear
(2) $\Rightarrow$ (1) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
(2) $\Rightarrow$ (3) Clear
(3) $\Rightarrow$ (2) $T_3(\mathbb{Z}/3\mathbb{Z})$ (the group of $3 \times 3$ upper triangular matrices with 1 on diagonal entries) is the Sylow 3-group of itself, thus nilpotent. But it is not abelian.
(3) $\Rightarrow$ (4) Let $|G| = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$, then $G \cong P_1 \times P_2 \times \cdots \times P_r$ where $P_i$ is a Sylow $p_i$-subgroup of $G$. Suppose $m = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r} | |G|$. By generalized first Sylow theorem, we have subgroups $Q_{p_i} \leq P_{p_i}$ of order $p_i^{e_i}$, and $Q_{p_1} \times Q_{p_2} \times \cdots \times Q_{p_n}$ gives a subgroup of $G$ of order $m$.
(4) $\Rightarrow$ (3) $S_3$ (If $S_3 \cong P_2 \times P_3$, then it is abelian).
(4) $\Rightarrow$ (5) Clear
(5) $\Rightarrow$ (4) $A_4$ has subgroups of order 3 and 4, but not of order 6.
(5) $\Rightarrow$ (6) Clear
(6) $\Rightarrow$ (5) $A_5$ has order 60 = $4 \cdot 15$ and $(4, 15) = 1$. If there is a subgroup $H$ of order 15, then
60 = |G| \mid (G : H)! = 4! shows that \( A_5 \) is not simple. This is a contradiction because we know that \( A_5 \) is simple!

8. Selected problems from Elman’s note

**Problem (4.17.12).** An even number \( N \) is perfect if and only if \( N = \frac{1}{2}p(p+1) \) with a Mersenne prime (so \( N = 2^{n-1}(2^n - 1) \) with \( p = 2^n - 1 \)).

**Proof.** If \( N = \frac{1}{2}p(p+1) \) with a prime \( p \), then

\[
\sigma(N) = \sigma(2^{n-1})\sigma(2^n - 1) = (2^n - 1)2^n = 2N
\]

On the other hand, suppose \( N \) is an even perfect number. We write \( N = 2^eM \) for odd \( M \) and \( e \geq 1 \). Since \( 2^{e+1}M = 2N = \sigma(N) = \sigma(2^e)\sigma(M) = (2^{e+1} - 1)M \), we have \( 2^{e+1} - 1 \mid M \). Let \( M = (2^{e+1} - 1)m \), then \( M > m \) since \( e > 0 \). Note that \( M \) and \( m \) are two distinct divisors of \( M \). Thus we have

\[
M + m \leq \sigma(M) = 2^{e+1}m = M + m
\]

The only way this is possible is that \( M \) is a prime and \( m = 1 \).

**Problem (8.5.1).** Let \( a, b \) be elements in a monoid such that \( ab \) has an inverse. Is it true that \( a \) and \( b \) have inverses? Prove this if true, give a counterexample if false.

**Proof.** False. Let \( M = \prod_{i=0}^{\infty} \mathbb{Z} \), and \( G = \text{End}(M) \). \( G \) is a monoid with the composition of functions. Consider \( f, g \in G \) defined by

\[
\begin{align*}
  f(a_0, a_1, a_2, \cdots) &= (0, a_0, a_1, \cdots) \\
g(a_0, a_1, a_2, \cdots) &= (a_1, a_2, a_3, \cdots)
\end{align*}
\]

Then \( gf = id_M \) has an inverse, but \( f \) does not have an (right) inverse since it is not surjective.

**Problem (11.9.10).** Let \( G \) and \( H \) be finite cyclic groups of order \( m \) and \( n \), respectively. Show the following.

1. If \( m \) and \( n \) are relatively prime, then \( \text{Aut}(G \times H) \cong \text{Aut}(G) \times \text{Aut}(H) \) and is abelian.
2. If \( m \) and \( n \) are not relatively prime, then \( \text{Aut}(G \times H) \) is never abelian.

**Proof.** (1) If \( m \) and \( n \) are relatively prime, then \( G \times H \) is cyclic of order \( mn \), and

\[
\text{Aut}(G \times H) \cong (\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times \cong \text{Aut}(G) \times \text{Aut}(H)
\]

(2) Assume \( G = \mathbb{Z}/m\mathbb{Z}, H = \mathbb{Z}/n\mathbb{Z} \) and \( \text{Aut}(G \times H) \) is abelian. Let \( d = (m, n) > 1 \) and \( m = dm', n = dn' \). Define \( \alpha, \beta \in \text{Aut}(G \times H) \) by \( \alpha(r, s) = (r + sn', s) \) and \( \beta(r, s) = (r, s + rm') \).

If \( \alpha\beta = \beta\alpha \), then

\[
(1 + m', 1 + n' + m'n') = \alpha\beta(1, 1) = \beta\alpha(1, 1) = (1 + m' + m'n', 1 + n')
\]

Thus \( m, n \mid m'n' \) and \( dm'n' = \text{lcm}(m, n) \mid m'n' \), which is a contradiction.

**Problem (18.26.2).** Let \( G \) be a group and \( \kappa(G) \) the number of conjugacy classes in \( G \). Suppose that \( G \) is finite. Show that \( \kappa(G) = 3 \) if and only if \( G \) is isomorphic to the cyclic group of order three or the symmetric group on three letters.
Proof. $k(\mathbb{Z}/3\mathbb{Z}) = \{1\} \cup \{2\} = 3 = \{1\}, \{(123), (132)\}, \{(12), (13), (23)\} = k(S_3)$.

Now suppose that $k(G) = 3$. We can write $G = C(1) \prod C(a) \prod C(b)$ for some $a, b \in G$ where $C(g)$ is the conjugacy class of $g$ in $G$. Let $m = |C(a)|, n = |C(b)|$ and assume $m \leq n$. We have $n = (G : Z_G(b)) | |G| = 1 + m + n$, thus $n | |G| - n = 1 + m$. So we get $m \leq n \leq m + 1$. If $m = 1$ and $n = 1$, then we have $|G| = 3$ and $G \cong \mathbb{Z}/3\mathbb{Z}$.

If $m = 1$ and $n = 2$, then $|G| = 4$ and thus $G$ is abelian. $G$ must have four conjugacy classes, so this case does not happen.

If $m \geq 2$ and $n = m$, then $m | |G| - 1 + 2m$. Contradiction!
If $m \geq 2$ and $n = m + 1$, then $m | |G| - m = 2 + m$. The only possible case is $m = 2, n = 3$, thus $|G| = 6$. Since $1_G \neq a \in Z_G(a)$ and $|Z_G(a)| = 3$, $a$ has order 3 in $G$. Similarly, $b$ has order 2 in $G$. Note that $a \notin C(b)$, which means $ab \neq ba$. Clearly $bab^{-1} \in C(a)$, and $a^2 \notin C(b)$ (otherwise we get from $ba^2 = a^2b$ to $ab = ba$). Thus $bab^{-1} = a^2$ and similarly we can show that $C(a) = \{a, bab^{-1} = a^2\}$ and $C(b) = \{b, aba^{-1} = ba, a^{-1}ba = ba^2\}$. Consider the following map $\lambda : G \to \Sigma(G/(b)) \cong S_3$ defined by $\lambda(g)(x(b)) = gx(b)$. We have $\ker \lambda \subseteq \langle b \rangle$ but $\langle b \rangle$ is not normal in $G$. $(aba^{-1} = ba \notin \langle b \rangle)$ Therefore, $\ker \lambda$ is trivial, and we conclude that $\lambda$ is an isomorphism by considering $|G| = |S_3|$.

\[ \bigcup_{g \in G} gHg^{-1} \subsetneq G \]

Proof. Note that we have a bijection between $\{gHg^{-1} \mid g \in G\}$ and $G/N_G(H)$ by $gHg^{-1} \leftrightarrow gN_G(H)$. Also we have $1_G \in gHg^{-1}$ for all $g \in G$.

\[
\left| \bigcup_{g \in G} gHg^{-1} \right| \leq (G : N_G(H))(|H| - 1) + 1 \\
\leq (G : H)(|H| - 1) + 1 \\
= |G| - (G : H) + 1 \leq |G|
\]

\[ \square \]

Problem (18.26.7). Suppose that $H$ is a proper subgroup of a finite group $G$. Show that

\[ \bigcup_{g \in G} gHg^{-1} \subsetneq G \]

Proof. Note that we have a bijection between $\{gHg^{-1} \mid g \in G\}$ and $G/N_G(H)$ by $gHg^{-1} \leftrightarrow gN_G(H)$. Also we have $1_G \in gHg^{-1}$ for all $g \in G$.

\[
\left| \bigcup_{g \in G} gHg^{-1} \right| \leq (G : N_G(H))(|H| - 1) + 1 \\
\leq (G : H)(|H| - 1) + 1 \\
= |G| - (G : H) + 1 \leq |G|
\]

\[ \square \]

Problem (19.11.1). Let $G$ be a finite group and $P$ be a Sylow $p$-subgroup. If $H$ is a subgroup of $G$ containing $N_G(P)$, then $H = N_G(H)$.

Proof. By \footnote{5.1} we have $N_G(H) = N_G(P)H \subseteq H$ since $H \subseteq N_G(H)$.

\[ \square \]

9. Some Examples

Example 9.1. Suppose that $G$ is a $p$-group with order $p^k$.

(1) If $n = 1$, then $G$ is simple and cyclic.
(2) If $n = 2$, then $G$ is not simple and abelian.
(3) If $n \geq 3$, then $G$ is not simple ($G$ has a nontrivial proper center or is abelian) and not necessarily abelian.

Example 9.2. It’s possible to have an element of odd order in a group which is a product of elements of even order. For example, in $D_5$, $r$ has order 5, but $r = s \cdot sr$ and $s, sr$ have order 2.
Example 9.3. Let \( G \) be a group and \( H \leq G, \ a \in G \). It’s possible to have \( aHa^{-1} \subseteq H \). For example, let \( G = GL_2(\mathbb{R}) \) and
\[
H = \left\{ \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \mid y \in \mathbb{Z} \right\} \cong \mathbb{Z}, \ a = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix},
\]
then
\[
aHa^{-1} = \left\{ \begin{pmatrix} 1 & 2y \\ 0 & 1 \end{pmatrix} \mid y \in \mathbb{Z} \right\} \subseteq H.
\]

10. Take Home Final

**Problem (1).** Let \( n \) be a positive integer relatively prime to \( \phi(n) \), and \( G \) a group of order \( n \). Show that \( G \) is cyclic, in the following steps. For this problem only you may assume the Feit-Thompson theorem: every finite group of odd order is solvable.

(1) Show that \( n \) has to be an odd squarefree integer. In other words, \( n = p_1p_2 \cdots p_s \) where \( p_1 < p_2 < \cdots < p_s \) are odd prime numbers.

(2) By Feit-Thompson, \( G \) is solvable. Show that it therefore has a cyclic quotient of prime order, that is, there is an epimorphism \( G \rightarrow H \) with \( H \) cyclic of prime order. Let \( N \) be the kernel.

(3) Show that \( G \cong N \times H \) and then prove that \( G \) is abelian.

(4) Now prove that \( G \) is cyclic.

**Proof.** Suppose \( |G| = n = 2^{e_0}p_1^{e_1}p_2^{e_2} \cdots p_r^{e_r} \) for \( p_1, p_2, \ldots, p_r \) odd primes and \( e_0 \geq 0, e_i \geq 1 \) for \( i \geq 1 \). Note that \( \phi(n) = 2^{e_0-1}p_1^{e_1-1}(p_1-1) \cdots p_r^{e_r-1}(p_r-1) \).

If \( e_0 \geq 1 \) and \( r \geq 1 \), then \( 2 \mid n, 2 \mid \phi(n) \). This cannot happen.

If \( n = 2^e \), then \( \phi(n) = 2^{e-1} \) and we should have \( e_0 = 1 \). Clearly, a group of order 2 is cyclic.

If \( e_0 = 0 \), then \( (n, \phi(n)) = 1 \) implies \( e_i = 1 \) for all \( i \), thus \( n = p_1p_2 \cdots p_r \) with odd primes \( p_1, p_2, \ldots, p_r \), and \( p_i \nmid p_j - 1 \) for all \( i, j \).

For the last case, we use induction on \( r \) to show that \( G \) is cyclic. By Feit-Thompson, \( G \) is solvable. Therefore, \( G \) has an abelian series. Without loss of generality, we can assume that we have a normal subgroup \( N \) of index \( (G : N) = p_s \). By induction hypothesis, \( N \) is cyclic. Choose \( a \in G \) of order \( p_s \) and let \( H = \langle a \rangle \). Let \( Syl_{p_s}(N) = \{ P_i \} \) for \( i = 1, 2, \ldots, s - 1 \). (\( N \) is abelian!) If \( Q \in Syl_{p_s}(G) \) and \( Q \cap N \) is trivial, we have \( p_s^2 = |Q||N| = |QN| |G| \). Therefore we must have \( Syl_{p_s}(G) = \{ P_i \} \). For each \( i \), \( HP_i \leq G \) is abelian because \( H \leq HP_i \) and \( P_i \leq HP_i \).

(Use the fact that \( p_i \nmid p_s - 1, p_i \nmid p_i - 1 \) and Sylow theorems.) Therefore \( H \) commutes with \( N = P_1P_2 \cdots P_{s-1} \cong P_1 \times P_2 \times \cdots \times P_{s-1} \), and \( G = HN \cong H \times N \) is cyclic. \( \square \)

**Problem (2).** Let \( G \) be a nontrivial finite solvable group and \( H \) a nontrivial normal subgroup not containing any other nontrivial normal subgroup of \( G \) properly. Show that there is a prime \( p \) and positive integer \( n \) such that \( H \cong (\mathbb{Z}/p\mathbb{Z})^n \).

**Proof.** Note that \( [H, H] \leq G \) because \( [g[h_1, h_2]g^{-1}] = [gh_1g^{-1}, gh_2g^{-1}] \in [H, H] \) for all \( g \in G \). ([\( h_1, h_2 \]) denotes the commutator \( h_1h_2h_1^{-1}h_2^{-1} \).) Since \( G \) is solvable, so is the subgroup \( H \). Thus \( [H, H] \leq H \), because otherwise the derived series of \( H \) would not converge to \( \{ 1 \} \). By assumption, \( [H, H] \) is trivial, and \( H \) is abelian. Choose a prime \( p \) such that \( p \mid |H| \). We have
\[
\{ 1 \} \leq H[p] = \{ h \in H \mid h^p = 1 \} \leq G
\]
since \( h^p = 1 \) implies \( (ghg^{-1})^p = gh^pg^{-1} = 1 \) for all \( g \in G \). Thus \( H = H[p] \) by assumption again, and \( H \cong (\mathbb{Z}/p\mathbb{Z})^n \) for some \( n \) since \( H \) is finite abelian and all nontrivial elements of \( H \) have order \( p \). \( \square \)
**Problem (3).** Let $G$ be a finite group, $n$ a positive integer and $\rho : G \to GL_n(\mathbb{R})$ a homomorphism. Show that there is a positive definite symmetric $n \times n$ matrix $A$ such that for all $g \in G$, $\rho(g)^t A \rho(g) = A$.

**Proof.** Define $A = \sum_{h \in G} \rho(h)^t \rho(h)$. For any $g \in G$, we have

$$\rho(g)^t A \rho(g) = \sum_{h \in G} \rho(g)^t \rho(h) \rho(h)^t \rho(g) = \sum_{h \in G} \rho(hg)^t \rho(hg) = A$$

Also we have $A^t = A$. For any nonzero vector $v \in \mathbb{R}^n$,

$$v^t A v = \sum_{h \in G} v^t \rho(h)^t \rho(h) v = \sum_{h \in G} |\rho(h)v|^2 > 0$$

which means $A$ is positive definite. \(\square\)

**References**


