1. Let $H$ be a subgroup of the symmetric group $S_n$ of index 2. Show that $H = A_n$. [Hint: Show that $H$ contains all squares of elements in $S_n$.]

Solution: The index $|S_n : H| = 2$, so $H \triangleleft S_n$. The quotient group $S_n/H$ has order 2 and therefore $(H\sigma)^2 = H1$ for all $\sigma \in S_n$. Thus $\sigma^2 \in H$ for all $\sigma \in S_n$.

In particular, $(\alpha \gamma \beta)^2 = (\alpha \beta \gamma)$, so $H$ contains all 3-cycles. The 3-cycles generate $A_n$ and hence $A_n \subseteq H$. However $|A_n| = |H| = \frac{1}{2}|S_n|$, so $H = A_n$.

2. Let $G$ be a finite group, let $p$ be a prime number and write $|G| = p^n m$ where $p$ does not divide $m$. The purpose of this question is to use group actions to show $G$ has a subgroup of order $p^n$; that is, $G$ has a Sylow $p$-subgroup.

(a) Let $\Omega$ be the collection of all subsets of $G$ of size $p^n$:

$$\Omega = \{ S \subseteq G \mid |S| = p^n \}.$$ 

Show that

$$|\Omega| = \binom{p^n m}{p^n} = m \left( \frac{p^n m - 1}{p^n - 1} \right) \left( \frac{p^n m - 2}{p^n - 2} \right) \cdots \left( \frac{p^n m - p^n + 2}{2} \right) \left( \frac{p^n m - p^n + 1}{1} \right).$$

(b) Let $j$ be an integer with $1 \leq j \leq p^n - 1$. Show that if the prime power $p^j$ divides $j$, then $p^j$ divides $p^n m - j$. Conversely show that if $p^j$ divides $p^n m - j$, then $p^j$ divides $j$.

Deduce that $|\Omega|$ is not divisible by $p$. [Examine each factor in the above formula and show that the power of $p$ dividing the numerator coincides with the power dividing the denominator.]

(c) Show that we may define a group action of $G$ on $\Omega$ by

$$\Omega \times G \rightarrow \Omega$$

$$(S, x) \mapsto Sx = \{ ax \mid a \in S \}.$$ 

(d) Express $\Omega$ as a disjoint union of orbits:

$$\Omega = \Omega_1 \cup \Omega_2 \cup \cdots \cup \Omega_k.$$ 

Show that $p$ does not divide $|\Omega_i|$ for some $i$.

(e) Let $S \in \Omega_i$ and let $P = G_S$, the stabiliser of $S$ in the action of $G$ on $\Omega$. Show that $p$ does not divide $|G : P|$ and deduce that $p^n$ divides $|P|$.

(f) Fix $a_0 \in S$. Explain why $a_0 x \in S$ for all $x \in P$. Show that $x \mapsto a_0 x$ is an injective map $P \rightarrow S$. Deduce that $|P| \leq p^n$.

(g) Conclude that $P$ is a Sylow $p$-subgroup of $G.$
Solution: (This is essentially the proof of a theorem broken down into parts, so we present the whole proof in one go.)

Let $\Omega$ be the set of all subsets of $G$ of size $p^n$. Then

$$|\Omega| = \binom{p^nm}{p^n} = \frac{p^n(m(p^n m - 1)(p^n m - 2) \ldots (p^n m - p^n + 1)}{p^n(p^n - 1)(p^n - 2) \ldots 2 \cdot 1} = m \left( \frac{p^n m - 1}{p^n - 1} \right) \left( \frac{p^n m - 2}{p^n - 2} \right) \ldots \left( \frac{p^n m - p^n + 2}{2} \right) \left( \frac{p^n m - p^n + 1}{1} \right). \quad (1)$$

To determine what power of $p$ divides $|\Omega|$, we first consider the rational number

$$\frac{p^n m - j}{j}$$

where $1 \leq j \leq p^n - 1$.

If $p^i$ divides $j$, then $i < n$ (since $j < p^n$), so $p^i$ also divides $p^n m - j$.

If $p^i$ divides $p^n m - j$, and $i \geq n$, then $p^n$ also divides $p^n m - j$ and hence divides $j$, contrary to the assumption that $j < p^n$. Thus, if $p^i$ divides $p^n m - j$ then $i < n$, so $p^i$ divides $p^n m$. Therefore $p^i$ divides $j = p^n m - (p^n m - j)$.

Hence the same power of $p$ divides $p^n m - j$ as divides $j$, so the numerator and the denominator of (1) are divisible by the same power of $p$. Therefore

$$|\Omega|$$

is not divisible by $p$.

Now let $G$ act on $\Omega$ by right multiplication:

$$\Omega \times G \rightarrow \Omega$$

$$(S, x) \mapsto Sx = \{ ax \mid a \in S \}.$$

We first note that since $a \mapsto ax$ is invertible, $|Sx| = |S| = p^n$ for all $S \in \Omega$, and hence if $S \in \Omega$ then $Sx \in \Omega$. Also, $(Sx)y = S(xy)$ and $S1 = S$. Hence this is an action of $G$ on $\Omega$. Write

$$\Omega = \Omega_1 \cup \Omega_2 \cup \cdots \cup \Omega_k$$

as a disjoint union of orbits. Then

$$|\Omega| = |\Omega_1| + |\Omega_2| + \cdots + |\Omega_k|.$$

Now $p$ does not divide $|\Omega|$, so one of the orbits has length not divisible by $p$. Let $i$ be such that $p$ does not divide $|\Omega_i|$, let $S \in \Omega_i$, and let $P = G_S$, the stabiliser of $S$ under this action:

$$P = \{ x \in G \mid Sx = S \}. \quad (2)$$
We will show that $P$ has order $p^n$ and hence is a Sylow $p$-subgroup. By the Orbit-Stabiliser Theorem:

$$|\Omega| = |G : P| = |G|/|P|,$$

so $|G : P|$ is not divisible by $p$. As $|G| = p^n m$, it follows that $p^n$ divides $|P|$. In particular, $|P| \geq p^n$.

Fix $a_0 \in S$. Equation (2) tells us that $Sx = S$ for all $x \in P$, so $a_0 x \in S$ for all $x \in P$. Hence we may define a map

$$\alpha : P \rightarrow S$$

$$x \mapsto a_0 x.$$  

This map is one-to-one (if $a_0 x = a_0 y$, then $x = a_0^{-1}(a_0 x) = a_0^{-1}(a_0 y) = y$), so $|P| \leq |S| = p^n$.

Hence $|P| = p^n$, and $P$ is a Sylow $p$-subgroup. This proves part (i) of Sylow’s Theorem.

3. Show that there is no simple group of order equal to each of the following numbers:

(i) 30; (ii) 48; (iii) 54; (iv) 66; (v) 72;
(vi) 84; (vii) 104; (viii) 132; (ix) 150; (x) 392.

[Note: These are not necessarily in increasing order of difficulty!]

Solution: (i) Let $G$ be a group of order $30 = 2 \cdot 3 \cdot 5$. Let $n_5$ be the number of Sylow 5-subgroups of $G$. Then, by Sylow’s Theorem,

$$n_5 \equiv 1 \pmod{5} \quad \text{and} \quad n_5 \mid 6.$$  

Therefore $n_5 = 1$ or 6. If $n_5 = 1$, then $G$ has a unique Sylow 5-subgroup, which is therefore normal in $G$, and $G$ is not simple.

Suppose then that $n_5 = 6$. A Sylow 5-subgroup has order 5 and hence any two distinct Sylow 5-subgroups intersect in the identity (by Lagrange’s Theorem). Therefore between them the Sylow 5-subgroups account for a total of $6 \times 4 = 24$ non-identity elements (all of which have order 5).

Therefore $G$ has 6 elements of order other than 5 (and these 6 include the identity element). Now let $n_3$ be the number of Sylow 3-subgroups of $G$. Then

$$n_3 \equiv 1 \pmod{3} \quad \text{and} \quad n_3 \mid 10$$

so $n_3 = 1$ or 10. But any two distinct Sylow 3-subgroups must also intersect in the identity (by Lagrange’s Theorem) and hence if $n_3 = 10$, then $G$ has
10 \times 2 = 20 \text{ elements of order 3}. \text{ We have now accounted for } 24 + 20 = 44 \text{ elements, contradicting the fact that } |G| = 30. \text{ Hence if } n_5 = 6 \text{ then } n_3 = 1.

Therefore a group of order 30 either has a normal Sylow 5-subgroup or a normal Sylow 3-subgroup, and is not simple.

(ii) Let $G$ be a group of order $48 = 2^4 \cdot 3$. Let $T$ be a Sylow 2-subgroup of $G$. Then $|G : T| = 3$. Let $G$ act by right multiplication on the cosets of $T$. This yields a homomorphism $\rho : G \to S_3$ with $\ker \rho \leq T$. Now $|G| > |S_3|$ so $\ker \rho \neq 1$, while $\ker \rho \neq G$ as $\ker \rho \leq T < G$. Hence $\ker \rho$ is a non-trivial proper normal subgroup of $G$, and $G$ is not simple.

(iii) Let $G$ be a group of order $54 = 2 \cdot 3^3$. Let $T$ be a Sylow 3-subgroup. Then $|T| = 27$, so $|G : T| = 2$ and therefore $T \leq G$. Thus $G$ is not simple.

(iv) Let $G$ be a group of order $66 = 2 \cdot 3 \cdot 11$. Let $n_{11}$ be the number of Sylow 11-subgroups of $G$. Then

$$n_{11} \equiv 1 \pmod{11} \quad \text{and} \quad n_{11} | 6,$$

so $n_{11} = 1$. Hence $G$ has a normal Sylow 11-subgroup, so is not simple.

(v) Let $G$ be a group of order $72 = 2^3 \cdot 3^2$. Let $n_3$ be the number of Sylow 3-subgroups of $G$. Then

$$n_3 \equiv 1 \pmod{3} \quad \text{and} \quad n_3 | 8,$$

so $n_3 = 1$ or 4. If $n_3 = 1$, then $G$ has a normal Sylow 3-subgroup, hence is not simple.

Suppose then that $n_3 = 4$. Let $T$ be a Sylow 3-subgroup of $G$ and let $H = N_G(T)$. Then, as the Sylow 3-subgroups of $G$ are the conjugates of $T$, we have


Let $G$ act by right multiplication on the right cosets of $H$. This yields a homomorphism $\rho : G \to S_4$ (since $|G : H| = 4$) with $\ker \rho \leq H$. Now $|G| > |S_4|$, so $\ker \rho \neq 1$. On the other hand, $\ker \rho \leq H < G$ and so $\ker \rho \neq G$. Hence if $n_3 = 4$, then $\ker \rho$ is a non-trivial proper normal subgroup of $G$, and so $G$ is not simple.

(vi) Let $G$ be a group of order $84 = 2^2 \cdot 3 \cdot 7$. Let $n_7$ be the number of Sylow 7-subgroups of $G$. Then

$$n_7 \equiv 1 \pmod{7} \quad \text{and} \quad n_7 | 12,$$

so $n_7 = 1$. Hence $G$ has a normal Sylow 7-subgroup, so $G$ is not simple.

(vii) Let $G$ be a group of order $104 = 2^3 \cdot 13$. Let $n_{13}$ be the number of Sylow 13-subgroups of $G$. Then

$$n_{13} \equiv 1 \pmod{13} \quad \text{and} \quad n_{13} | 8,$$
so $n_{13} = 1$. Hence $G$ has a normal Sylow 13-subgroup, so is not simple.

(viii) Let $G$ be a group of order $132 = 2^2 \cdot 3 \cdot 11$. Let $n_{11}$ be the number of Sylow 11-subgroups of $G$. Then

$$n_{11} \equiv 1 \pmod{11} \quad \text{and} \quad n_{11} \mid 12,$$

so $n_{11} = 1$ or 12. If $n_{11} = 1$, then $G$ has a normal Sylow 11-subgroup, so is not simple.

Suppose that $n_{11} = 12$. Since the Sylow 11-subgroups have order 11, Lagrange’s Theorem shows that any two of them intersect in the identity, so the Sylow 11-subgroups contain a total of $12 \times 10 = 120$ elements of order 11.

Now let $n_3$ be the number of Sylow 3-subgroups of $G$. Then

$$n_3 \equiv 1 \pmod{3} \quad \text{and} \quad n_3 \mid 44,$$

so $n_3 = 1, 4$ or 22. If $n_3 = 1$, then $G$ has a normal Sylow 3-subgroup, so is not simple. Any two distinct Sylow 3-subgroups intersect in the identity (they have order 3), and hence $G$ contains $2n_3$ elements of order 3. However, there only remain $12 (= 132 - 120)$ elements of order not equal to 11 in $G$. Thus $n_3 = 4$, and therefore $G$ has 8 elements of order 3.

There are only 4 remaining elements in $G$ (not of order 3 or 11). These must include all the elements of all the Sylow 2-subgroups, and hence $G$ has only one Sylow 2-subgroup if $n_3 \neq 1$ and $n_{11} \neq 1$.

In conclusion, for one of $p = 2, 3$ or 11, $G$ has a normal Sylow $p$-subgroup, and so is not simple.

(ix) Let $G$ be a group of order $150 = 2 \cdot 3 \cdot 5^2$. Let $F$ be a Sylow 5-subgroup of $G$, so that $|G : F| = 6$. Let $G$ act by right multiplication on the cosets of $F$, yielding a homomorphism $\rho: G \to S_6$ with $\ker \rho \leq F$. Certainly $\ker \rho \neq G$ since $\ker \rho \leq F$. If $\ker \rho = 1$, then $G \cong \im \rho \leq S_6$. Thus $|\im \rho| = 150$, yet 150 does not divide 6! (as $5^2$ does not divide 6!). Therefore $\ker \rho \neq 1$, and $\ker \rho$ is a non-trivial proper normal subgroup of $G$. Hence $G$ is not simple.

(x) Let $G$ be a group of order $392 = 2^3 \cdot 7^2$. Let $S$ be a Sylow 7-subgroup of $G$, so that $|G : S| = 8$. Let $G$ act by right multiplication on the cosets of $S$, yielding a homomorphism $\rho: G \to S_8$ with $\ker \rho \leq S$. Certainly $\ker \rho \neq G$ since $\ker \rho \leq S$. If $\ker \rho = 1$, then $G \cong \im \rho \leq S_8$. Then $|\im \rho| = 392$, yet 392 does not divide 8! (as $7^2$ does not divide 8!). Thus $\ker \rho \neq 1$, and $\ker \rho$ is a non-trivial proper normal subgroup of $G$. Hence $G$ is not simple.

4. Let $G$ be a finite group, $N$ be a normal subgroup of $G$ and $P$ be a Sylow $p$-subgroup of $G$.

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

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

[Hint: Show that the subgroup is of order a power of $p$ and has index not divisible by $p$. In both parts expect to use the formula for the order of $PN$ and the fact that $P$ already has the required property as a subgroup of $G$.]
Solution:  \( P \cap N \) is a subgroup of \( P \), so \( P \cap N \) is a \( p \)-subgroup of \( N \). Also, \( N \trianglelefteq G \) implies that \( PN \) is a subgroup of \( G \). Now
\[
|PN| = |P| \cdot |N|/|P \cap N|,
\]
so
\[
|N : P \cap N| = |N|/|P \cap N| = |PN|/|P| = |PN : P|.
\]
Now \( P \) is a Sylow \( p \)-subgroup of \( G \), so it is also a Sylow \( p \)-subgroup of \( PN \trianglelefteq G \). Hence \( p \) does not divide \( |PN : P| \). Thus \( P \cap N \) is a \( p \)-subgroup of \( N \) whose index is not divisible by \( p \); that is, \( |P \cap N| \) is the largest power of \( p \) dividing \( |N| \). Therefore \( P \cap N \) is a Sylow \( p \)-subgroup of \( N \).

(b) Here
\[
|PN/N| = |PN|/|N| = |P|/|P \cap N|.
\]
Hence \( PN/N \) is a \( p \)-subgroup of \( G/N \). Furthermore,
\[
|G/N : PN/N| = \frac{|G/N|}{|PN/N|} = \frac{|G|/|N|}{|P|/|P \cap N|} = \frac{|G : P|}{|N : N \cap P|}.
\]
Since \( p \) does not divide the numerator of the final fraction, \( p \) does not divide the index of \( PN/N \) in \( G/N \). Hence \( PN/N \) is a Sylow \( p \)-subgroup of \( G/N \).

5. Let \( G \) be a finite group, \( p \) be a prime number dividing the order of \( G \), and let \( P \) be a Sylow \( p \)-subgroup of \( G \). Define
\[
O_p(G) = \bigcap_{g \in G} P^g.
\]
Show that \( O_p(G) \) is the largest normal \( p \)-subgroup of \( G \).

Solution:  Each conjugate of \( P \) is a subgroup of \( G \). Therefore \( O_p(G) \) is an intersection of subgroups, so is a subgroup of \( G \). By Lagrange’s Theorem, \( |O_p(G)| \) divides \( |P| \), so \( O_p(G) \) is a \( p \)-subgroup of \( G \).

Conjugation permutes the conjugates of \( P \), so \( O_p(G) \) is a normal subgroup of \( G \). [To see this: let \( x \in O_p(G) \) and \( h \in G \). Consider any conjugate \( P^g \) of \( P \). Then \( x \in O_p(G) \) \( \leq P^{gh^{-1}} \) (as this is a conjugate of \( P \)) so \( x^h \in P^g \) for all \( g \in G \). Thus \( x^h \in O_p(G) \) for all \( x \in O_p(G) \) and \( h \in G \); that is, \( O_p(G) \leq G \).]

Let \( K \) be any normal \( p \)-subgroup of \( G \). By Sylow’s Theorem, \( K \) is contained in one of the Sylow \( p \)-subgroups of \( G \); say, \( K \leq P^h \) for some \( h \in H \). Then
\[
K = K^{h^{-1}} \leq P
\]
so
\[
K = K^g \leq P^g \quad \text{for all } g \in G.
\]
Hence
\[
K \leq \bigcap_{g \in G} P^g = O_p(G).
\]
This shows that \( O_p(G) \) is the largest normal \( p \)-subgroup of \( G \).