1. Let $G$ be a finite group and, for each prime $p$, choose a $p$-Sylow subgroup of $G$. Prove that $G$ is generated by these subgroups (that is every element of $G$ is expressible as a product of some elements of these subgroups.) **Solution:**

Let $H$ be the subgroup of $G$ generated by the chosen Sylow subgroups. For every prime $p$ dividing the order of $G$, $H$ has a $p$-Sylow subgroup of $G$ as a subgroup. Hence, $|H|$ is divisible by the maximum power of $p$ dividing $|G|$. Hence, $H = |G|$ which implies that $H = G$.

2. If $p$ and $q$ are primes, prove that a group of order $p^2q$ cannot be simple. **Solution:**

Let $G$ be a group with $|G| = p^2q$. Assume $p \neq q$.

Otherwise, $|G| = p^3$ and $G$ has a normal subgroup of order $p^2$.

Assume that $G$ is simple.

The number of $p$-Sylow subgroups must be $q$ and hence $q = 1 \mod p$. Hence, $q > p$.

The number of $q$-Sylow subgroups is either $p$ or $p^2$. It cannot be $p$, because this would imply that $p = 1 \mod q$ implying $p > q$.

Hence, the number of $q$-Sylow subgroups must be $p^2$. But any pair of these subgroups can have only the identity as a common element. Hence, the total number of non-identity elements in the $q$-Sylow subgroups is $p^2(q - 1)$. On the other hand the intersection any two distinct $p$-Sylow subgroup can have size at most $p$ (the intersection has to be a subgroup of each). Thus, the number of elements in the $p$-Sylow subgroups is at least $2p^2 - p$.

But then, $p^2(q - 1) + 2p^2 - p = p^2q + p(p - 1) > p^2q$ which is a contradiction.

3. Let $G$ be a finite group with an automorphism $\varphi$ such that $\varphi(x) = x$ if and only if $x = e$.

   (a) Show that every element of $G$ can be written as $x^{-1}\varphi(x)$.

   (b) Suppose $\varphi$ has order two, i.e., $\varphi^2(x) = x$ for all $x \in G$. Prove that $\varphi(x) = x^{-1}$ for all $x \in G$, and conclude that $G$ is abelian.

**Solution:** (a) If $x^{-1}\varphi(x) = y^{-1}\varphi(y)$, then $yx^{-1} = \varphi(yx^{-1})$, and so we must have $yx^{-1} = e$, i.e., $y = x$. Consequently the map $f : G \to G$ with $f(x) = x^{-1}\varphi(x)$ is injective. Since $G$ is finite, it must be surjective as well.

   (b) Note that

   $$\varphi(y^{-1}\varphi(y)) = \varphi(y^{-1})\varphi(y) = \varphi(y^{-1})y = (y^{-1}\varphi(y))^{-1}.$$ 

   Since every element $x \in G$ has the form $y^{-1}\varphi(y)$, it follows that $\varphi(x) = x^{-1}$ for all $x \in G$.

4. Let $p < q$ be prime numbers such that $p$ divides $q - 1$. Show that there exists a non-abelian group of order $pq$. 

1
Solutions to Assignment 3

Solution: Let $P = \mathbb{Z}/\langle p \rangle$ and $Q = \mathbb{Z}/\langle q \rangle$. Then $|\text{Aut}(Q)| = q - 1$, and since $p|(q - 1)$, there exists $\varphi \in \text{Aut}(Q)$ with $|\varphi| = p$. Consequently we have a non-trivial homomorphism

$$\alpha : P \longrightarrow \text{Aut}(Q) \quad \text{where} \quad \alpha(n \mod p) = \varphi^n \quad \text{for} \quad 0 \leq n \leq p - 1.$$ 

The semi-direct product $G = Q \rtimes_P P$ is a nonabelian group of order $pq$.

5. Let $p, q$ be distinct prime numbers. Prove that a group of order $p^2q$ is solvable.

Solution: Let $|G| = p^2q$ and $P$ and $Q$ be $p$-Sylow and $q$-Sylow subgroups respectively. Note that $P$ and $Q$ are abelian. Let $s_p$ and $s_q$ be the number of distinct $p$-Sylow and $q$-Sylow subgroups respectively. Since the conjugation action of $G$ is transitive on the set of $p$-Sylow subgroups, we have $s_p = (G : N_P)$. This implies that $s_p|q$, and a similar argument shows that $s_q|p$.

If $s_p = 1$, then $\{e\} \triangleleft P \triangleleft G$ is an abelian tower for $G$, so for the rest of the proof we may assume $s_p = q$. Since $s_p \equiv 1 \mod p$, we note that $p|(q - 1)$.

If $s_q = 1$, then $\{e\} \triangleleft Q \triangleleft G$ is an abelian tower for $G$. The remaining cases are $s_q = p$ and $s_q = p^2$. Since $s_q \equiv 1 \mod q$, we have $q|(p^2 - 1)$ in either case.

Since $p|(q - 1)$, we may write $q = kp + 1$ for some positive integer $k$. But then $q = kp + 1$ divides $(p^2 - 1) = (p - 1)(p + 1)$, and the only possibility is $q = kp + 1$ divides $p + 1$, and so $k = 1$. Therefore in the remaining case we must have $p = 2$ and $q = 3$. But then $|G| = 12$, and we have observed in class that at least one of the Sylow subgroups of a group of order 12 is normal.

6. Let $G$ be a finite group, $K \triangleleft G$ a normal subgroup, and $P$ a $p$-Sylow subgroup of $K$. Prove that $G = KN_P$, where $N_P$ is the normalizer of $P$ in $G$.

Solution: Let $g \in G$. Then $gPg^{-1} < gKg^{-1} = K$, and so $gPg^{-1}$ is a $p$-Sylow subgroup of $K$. Since $p$-Sylow subgroups of $K$ are conjugate, there exists $k \in K$ such that $kPk^{-1} = gPg^{-1}$. But then $P = k^{-1}gPg^{-1}k$, and so $k^{-1}g \in N_P$. It follows that $g \in KN_P$ but, since $g$ was an arbitrary element of $G$, we get $G = KN_P$.

7. Let $|G| = p^km$ where $p$ is a prime number. Let $S$ be the set of $p^k$-element subsets of $G$, and so

$$|S| = \binom{p^km}{p^k}, \quad \text{and therefore} \quad \frac{|S|}{m} = \binom{p^km - 1}{p^k - 1}.$$ 

(a) Show that $(1/m)|S| \equiv 1 \mod p$.

(b) Let $G$ act on $S$ by left translation. If $A \in S$, prove that the order of the isotropy group $G_A$ divides $p^k$.

(c) Let $S_0 = \{A \in S : |G_A| = p^k\}$, and show that

$$|S| \equiv |S_0| \mod pm.$$ 

(Hint: Note that $S \setminus S_0$ is a disjoint union of orbits.)
Solutions to Assignment 3

(d) Prove that \( S_0 = \{ Hx : H \text{ is a subgroup of } G \text{ with } |H| = p^k, \text{ and } x \in G \} \).

(e) Conclude that the number of subgroups of \( G \) of order \( p^k \) is \( 1 \mod p \). (This extends the Sylow theorems, since we did not assume that \( m \) is relatively prime to \( p \).)

Solution: (a) Note that we can write the binomial coefficient as a product

\[
\binom{p^k m - 1}{p^k - 1} = \frac{p^k m - 1}{p^k - 1} \cdots \frac{p^k m - i}{p^k - i} \cdots \frac{p^k m - (p^k - 1)}{p^k - (p^k - 1)}.
\]

An integer \( 1 \leq i \leq p^k - 1 \) can be written as \( i = p^r t \) with \( (p, t) = 1 \) and \( r < k \). Since

\[
\frac{p^k m - i}{p^k - i} = \frac{p^k m - p^r t}{p^k - p^r t} = \frac{p^k - r m - t}{p^k - r - t} \equiv 1 \mod p,
\]

we get

\[
\binom{p^k m - 1}{p^k - 1} \equiv 1 \mod p.
\]

(b) The isotropy group \( G_A \) acts on the set \( A \) by left translation. The orbit of an element \( x \in A \) is the right coset \( G_A x \), which has \( |G_A| \) elements. Consequently

\[
|A| = p^k = |G_A| \quad \text{(number of orbits for the action of } G_A \text{ on } A).
\]

(c) Let \( A_i \) and \( B_j \in S \) be representatives for orbits of the action of \( G \) on \( S \), such that \( |G_{A_i}| = p^k \) for all \( i \in I \), and \( |G_{B_j}| < p^k \) for all \( j \in J \). The set \( S_0 \) if the union of the orbits of \( A_i \) for \( i \in I \), and the set \( S \setminus S_0 \) if the union of the orbits of \( B_j \) for \( j \in J \). By (b), \( |G_{B_j}| \) is a power of \( p \) and since \( |G_{B_j}| < p^k \), we get \( pm | (G : G_{B_j}) \). This implies that \( pm \) divides

\[
\sum_{j \in J} (G : G_{B_j}) = |S \setminus S_0|.
\]

(d) If \( H \) is a subgroup of order \( p^k \), then the isotropy group of the right coset \( Hx \) is

\[
G_{Hx} = \{ g \in G : gHx = Hx \} = H,
\]

and so \( Hx \in S_0 \).

Conversely, if \( |G_A| = p^k \) for \( A \in S \), then for an element \( a \in A \) we have \( G_A a \subseteq A \). Since each of these sets have \( p^k \) elements, it follows that \( G_A a = A \).

(e) Let \( n \) be the number of subgroups of \( G \) of order \( p^k \). Such a subgroup has index \( m \), and since \( S_0 \) is the set of right cosets of subgroups of order \( p^k \), we have \( |S_0| = nm \). By (c) and (a),

\[
nm \equiv |S| \equiv m \mod pm,
\]

and so \( n \equiv 1 \mod p \).

8. Let \( K \) be an abelian group of order \( m \) and let \( Q \) be an abelian group of order \( n \). If \( (m, n) = 1 \), then every extension \( G \) of \( K \) by \( Q \) is a semi-direct product.

Solution explained in class.