1. Let H and K be finite subgroups of a group G.

   (a) Recall that $HK = \{hk : h \in H, k \in K\}$, and show
   $$|HK| = \frac{|H||K|}{|H \cap K|}.$$

   (b) For $x \in G$, the set $HxK = \{hxk : h \in H, k \in K\}$ is called a *double coset* of H and K. Show that G is a disjoint union of double cosets and
   $$|HxK| = \frac{|H||K|}{|H \cap xKx^{-1}|}.$$

   (c) If all double cosets of the form HxH for $x \in G$ have the same number of elements, show that $H \lhd G$.

   Solution: (a) follows from (b) using $x = e$.

   (b) If HxK and HyK are two double cosets and $hxk \in HyK$ for $h \in H$ and $k \in K$, then $x \in HyK$, and so $HxK \subseteq HyK$. Consequently HxK and HyK are either disjoint or equal.

   Next note that xKx^{-1} is a subgroup of G, and so $H \cap xKx^{-1}$ is a subgroup of H. Therefore H is the disjoint union of left cosets of $H \cap xKx^{-1}$, i.e.,
   $$H = \bigcup_{i \in I} h_i(H \cap xKx^{-1})$$
   where I is a finite index set, $h_i \in H$, and the union is disjoint. But then
   $$HxK = \bigcup_{i \in I} h_i xK. \qquad (*)$$
   The cosets $\{h_i xK\}_{i \in I}$ are left cosets of K, and so they must be equal or disjoint. If $h_i xK = h_j xK$, then $x^{-1}h_j^{-1}h_i x \in K$, and $h_j^{-1}h_i \in H \cap xKx^{-1}$. This implies $h_i = h_j$, and so we have a disjoint union in $(*)$. Consequently
   $$|I| = \frac{|H|}{|H \cap xKx^{-1}|} = \frac{|HxK|}{|xK|} = \frac{|HxK|}{|K|}.$$

   (c) If $|HxH|$ does not depend on x, then $|HxH| = |HeH| = |H|$ for all $x \in G$. The formula from (b) now implies that $|H| = |H \cap xHx^{-1}|$, i.e., that $xHx^{-1} = H$ for all $x \in G$.

2. Let G be a p-group where p be a prime integer.

   (a) If $|G| = p^2$, show that G is abelian.

   (b) If $|G| = p^3$, show that either G is abelian or $|Z(G)| = p$, where $Z(G)$ is the center of G.

   Solution: We set $Z = Z(G)$. Since G is a p-group, p divides $|Z|$. Suppose G/Z is cyclic, then there exists $a \in G$ such that aZ generates the group G/Z. Consequently $G = \bigcup a^n Z$, and so every element of G has the form $a^n z$ for some integer n and $z \in Z$. It follows that G is abelian.

   (a) In this case G/Z can have order 1 or p, so it must be cyclic. Consequently G is abelian (and so $G = Z$).

   (b) We must have $|Z| \in \{p, p^2, p^3\}$. If $|Z| \neq p$, then $|G/Z| \in \{1, p\}$ so G/Z is cyclic, and therefore G is abelian.

3. Let p be a prime integer and G be a p-group. If $H \lhd G$ and $|H| = p$, prove that H is contained in the center of G.

   Solution: Since H is normal G acts on H by conjugation, and this gives us a homomorphism

   $$\phi : G \longrightarrow \mathrm{Aut}(H).$$

   But $|\mathrm{Aut}(H)| = p - 1$, and so $|\mathrm{Image}(\phi)| = 1$. Consequently $\mathrm{Image}(\phi)$ is the trivial automorphism, i.e., $xhx^{-1} = h$ for all $h \in H$ and $x \in G$.

4. Let G be an infinite group and H a subgroup of finite index. Show that G has a normal subgroup K of finite index, with $K < H$.

   Solution: Let S be the set of left cosets of H and $n = |S| = (G : H)$. Then G acts by translation on S,

   $$\phi : G \longrightarrow \mathrm{Perm}(S), \qquad g \mapsto (xH \mapsto gxH).$$

   Let $K = \mathrm{Ker}\,\phi$. Then $K \lhd G$ and $|G/K|$ divides $n!$ and so K has finite index in G. If $k \in K$ then $kxH = xH$ for all $x \in G$, and so $k \in H$.

5. Let G be an infinite group containing an element $x \neq e$ having only finitely many conjugates. Prove that G is not simple.

   Solution: Let G act on itself by conjugation. The orbit of x is finite, so $(G : G_x) < \infty$ where G_x is the isotropy group of x. By (4), there exists a subgroup $K \lhd G$ of finite index, with $K < G_x$. Consequently if $G_x \neq G$, then $K \neq G$ is a nontrivial normal subgroup, and so G is not simple.

   If $G_x = G$ then $x \in Z(G)$, and so $Z(G) \lhd G$ is a nontrivial normal subgroup; if $Z(G) \neq G$ it follows that G is not simple. If $Z(G) = G$, then G is an infinite abelian group and we claim such a group cannot be simple: Let $g \in G$ where $g \neq e$. Then $\langle g \rangle \lhd G$ and so, if G is simple, $\langle g \rangle = G$, i.e., G is an infinite cyclic group with generator g. But then $\langle g^2 \rangle \lhd G$ is a nontrivial proper normal subgroup, contradicting the assumption that G is simple.

6. Let G be a finite group such that $\mathrm{Aut}(G)$ acts transitively on the set $G \setminus \{e\}$. Show that G is a p-group for some prime p, and that G is abelian.

   Solution: Let p be a prime dividing $|G|$. Then there exists $x \in G$ with $|x| = p$. Let $y \in G \setminus \{e\}$ be an arbitrary element. Then there exists $\phi \in \mathrm{Aut}(G)$ with $\phi(x) = y$, and so $e = \phi(x^p) = y^p$, which implies that $|y| = p$. Consequently if $q \neq p$ is a prime, then G has no elements of order q, and so $|G|$ must be a power of p.

   Since G is a p-group, there exists $z \neq e$ in the center of G. If $a, b \in G \setminus \{e\}$ are arbitrary elements, then there exists $\psi \in \mathrm{Aut}(G)$ with $\psi(b) = z$. But then

   $$\psi(ab) = \psi(a)z = z\psi(a) = \psi(ba).$$

   Since ψ is an automorphism, and hence injective, $ab = ba$.

7. Let G be a group with $|G| = mp^n$ where p is a prime and $m < p$. Show that G has exactly one p-Sylow subgroup, and that this subgroup is normal.

   Solution: We saw that G acts on the set of p-Sylow subgroups by conjugation, and that this action is transitive. Let P be any p-Sylow subgroup. Then the number of p-Sylow subgroups is the length of the orbit of P, which equals $(G : G_P)$, where G_P is the isotropy group of P. Note

that $P < G_p < G$, and so $(G : G_P)$ divides $(G : P) = m$. Consequently the number of p-Sylow subgroups divides m, and is also $1 \mod p$. Since $m < p$, there is only one p-Sylow subgroup, namely P. Since xPx^{-1} is also a p-Sylow subgroup, we must have $xPx^{-1} = P$ for all $x \in G$, i.e., $P \lhd G$.

8. Let G be a finite group of odd order which acts transitively on a set S. For $s \in S$, show that the orbits of the action of G_s on $S \setminus \{s\}$ have lengths which are equal in pairs.

   Solution: Let $H = G_s$. Since the action of G on S is transitive, every element of S is of the form ys for $y \in G$, and so every element of $S \setminus \{s\}$ is of the form ys for $y \notin H$. We claim that for $y \notin H$, the orbits of ys and $y^{-1}s$ under the action of H are disjoint and have the same length.

   Suppose $hys = y^{-1}s$ for $h \in H$, then $yhys = s$, i.e., $yhy \in H$. In that case, $(yh)^2 \in H$. Since $|G|$ is odd, $|yh|$ must be an odd integer, say $2k+1$. But then

   $$yh = yh(yh)^{2k+1} = \left((yh)^2\right)^{k+1} \in H,$$

   which contradicts the assumption that $y \notin H$. This proves that ys and $y^{-1}s$ belong to disjoint orbits under the action of H.

   The length of the orbit of ys under the action of H is $(H : H_{ys})$, where

   $$H_{ys} = \{h \in H : hys = ys\} = \{h \in H : y^{-1}hy \in H\} = H \cap yHy^{-1}.$$

   is the isotropy subgroup of ys. Therefore the length of the orbit of ys under the action of H is

   $$|H|/|H \cap yHy^{-1}|.$$

   Similarly, the length of the orbit of $y^{-1}s$ under the action of H is

   $$|H|/|H \cap y^{-1}Hy|,$$

   and these lengths are equal since

   $$|H \cap y^{-1}Hy| = |y\left(H \cap y^{-1}Hy\right)y^{-1}| = |yHy^{-1} \cap H|.$$

9. Let G be a finite group and p a prime number. An element $g \in G$ is called *p-unipotent* if its order is a power of p, and *p-regular* if its order is not divisible by p.

   (a) Let $x \in G$. Show that there exists a unique ordered pair (u, r) of elements of G such that u is p-unipotent, r is p-regular, and $x = ur = ru$.

   (Hint: First consider the case where G is the cyclic group generated by x.)

   (b) Let P be a p-Sylow subgroup of G, C the centralizer of P, and E the set of p-regular elements of G. Show that

   $$|E| \equiv |E \cap C| \mod p.$$

   (c) Deduce that p does not divide the order of E.

   (Hint: Use induction on the cardinality of G to reduce to the case where $C = G$; then use (a)).

Solution: (a) Let U be the set of p-unipotent elements of G, and E the set of p-regular elements. Note that $U \cap E = \{e\}$ and that U is a subgroup whenever the elements of U commute; likewise, E is a subgroup whenever the elements of E commute.

We first consider the case $G = \langle x \rangle$. Since G is abelian in this case, U and E are both subgroups of G. Consequently if $x = ur = u'r'$ for $u, u' \in U$ and $r, r' \in E$, then $u'^{-1}u = r'r^{-1} \in U \cap E = \{e\}$, and so $u = u'$ and $r = r'$.

Let $|x| = mp^n$ where m and p are relatively prime. There exist positive integers $a, b \in \mathbb{Z}$ such that $am + bp^n \equiv 1 \mod mp^n$. Note that this implies $(a, p^n) = 1$ and $(b, m) = 1$. We have

$$x = x^{am+bp^n} = x^{am}x^{bp^n} = ur$$

where $u = x^{am}$ has order p^n and $r = x^{bp^n}$ has order m.

If G is not necessarily cyclic, we still have $x = ur = ru$ for a p-unipotent element $u \in \langle x \rangle$ and a p-regular element $r \in \langle x \rangle$. Suppose $x = u'r' = r'u'$ is another such factorization with $u' \in U$ and $r' \in E$. Then $u' = xr'^{-1}$ and so $x = r'xr'^{-1}$, i.e., $xr' = r'x$. Similarly $xu' = u'x$, and so u' and r' commute with x, and hence also with u and r which are powers of x. But then $u'^{-1}u = r'r^{-1} \in U \cap E = \{e\}$, and so uniqueness follows in the general case as well.

(b) Since conjugation preserves the order of an element, P acts on E by conjugation. The fixed points of this action are precisely the elements of $E \cap C$. Since P is a p-group, it follows that $|E| \equiv |E \cap C| \mod p$.

(c) We use induction on $|G|$. The result is certainly true if $|G| = p$. The set of p-regular elements of C is precisely $|E \cap C|$, and so if C is a proper subgroup of C, the induction hypothesis implies that p does not divide $|E \cap C|$. Using (b), it then follows that p does not divide $|E|$.

Consequently we may assume that $C = G$, i.e., that P is in the center of G. This implies, in particular, that $P \lhd G$, and so P is the unique p-Sylow subgroup of G, and $P = U$. In this case, consider the map

$$f : U \times E \to G \qquad \text{where} \qquad f(u, r) = ur = ru.$$

By (a), this map is a bijection, and so $|G| = |U||E|$. Since $U = P$ is a p-Sylow subgroup of G, we conclude that p does not divide $|E|$.

10. Let G be a finite group, P a Sylow subgroup of G, and N the normalizer of P. Let X_1 and X_2 be subsets of the center of P which are conjugate, i.e., $sX_1s^{-1} = X_2$ for some element $s \in G$.

    (a) Show that there exists $n \in N$ such that $nxn^{-1} = sxs^{-1}$ for all $x \in X_1$.

    (b) Deduce that two elements of the center of P are conjugate in G if and only if they are conjugates in N.

Solution: (a) Let C be the centralizer of X_1 in G. Since $X_1 < Z(P)$, it follows that P is contained in C, and hence that P is a Sylow subgroup of C. Since $X_2 = sX_1s^{-1} \subseteq Z(P)$, it is easily checked that $X_1 \subseteq Z(s^{-1}Ps)$, and so $s^{-1}Ps$ is also contained in C. But Sylow subgroups of C are conjugate, so there exists $t \in C$ such that $s^{-1}Ps = tPt^{-1}$. Consequently $P = stPt^{-1}s^{-1}$, and so $n = st \in N$. Now if $x \in X_1$, then $nxn^{-1} = stxt^{-1}s^{-1} = sxs^{-1}$ since $t \in C$.

(b) follows immediately from (a), taking X_1 and X_2 to be the appropriate singleton sets.