II.5.2

If G is a finite p-group, $H \lhd G$ and $H \neq \langle e \rangle$, then $H \cap C(G) \neq \langle e \rangle$.

Proof. Let H be a nontrivial normal subgroup of G. Then we have that for each conjugacy class C of G, either $C \subseteq H$ or $C \cap H = \emptyset$ because H is normal. Pick representatives of the conjugacy classes of G:

$$a_1, a_2, \ldots, a_r,$$

with $a_1, \ldots, a_k \in H$ and $a_{k+1}, \ldots, a_r \notin H$. Let C_i be the conjugacy class of a_i in G, for all i. Thus,

$$C_i \subseteq H, \quad i = 1, 2, \ldots, k, \quad \text{and} \quad C_i \cap H = \emptyset, \quad i = k+1, k+2, \ldots, r.$$

By renumbering $a_1, \ldots, a_k$ if necessary, we may assume $a_1, \ldots, a_s$ represent classes of size 1 (i.e., are in the center of G) and $a_{s+1}, \ldots, a_k$ represent classes of size greater than 1. Since H is the disjoint union of these we have that

$$|H| = |H \cap C(G)| + \sum_{i=s+1}^{k} \frac{|G|}{|C_G(a_i)|}.$$

Now p divides $|H|$ and p divides each term in the sum $\sum_{i=s+1}^{k} [G : C_G(a_i)]$. So p divides their difference: $|H \cap C(G)|$. This proves $H \cap C(G) \neq \langle e \rangle$. If $|H| = p$, since $H \cap C(G) \neq \langle e \rangle$, we must have $H \leq C(G)$. □

II.5.5

If P is a normal Sylow p-subgroup of a finite group G and $f : G \to G$ is an endomorphism, then $f(P) \leq P$.

Proof. Since P is a Sylow p-subgroup of G, we know that $|P| = p^k$ for some integer $k \geq 0$, and that P is maximal with respect to this property. Since P is normal in G, we have that for any $g \in G$, the conjugate $gPg^{-1} = P$.

Now, consider the endomorphism $f : G \to G$. The image of P under f, denoted by $f(P)$, is a subgroup of G. We need to show that $f(P) \leq P$.

First, note that since f is a homomorphism, it preserves the group operation. Therefore, for any elements $x, y \in P$, we have

$$f(xy) = f(x)f(y).$$

This shows that the image of the product of two elements in P is the product of their images, which means that $f(P)$ is closed under the group operation.

Next, we need to show that the order of $f(P)$ divides the order of P. Since P is a finite group of order p^k, any subgroup of P must have an order that is a power of p. Therefore, the order of $f(P)$ must be of the form p^m for some integer $m \leq k$.

Now, since P is normal in G, for any element $g \in G$, we have

$$gf(P)g^{-1} = f(gPg^{-1}) = f(P),$$

which shows that $f(P)$ is also normal in G.

Finally, since both P and $f(P)$ are Sylow p-subgroups of G, and Sylow's theorems state that all Sylow p-subgroups are conjugate to each other (Second Sylow Theorem), it follows that there exists some element $g \in G$ such that

$$f(P) = gPg^{-1}.$$

However, since P is normal in G, we have

$$gPg^{-1} = P.$$

Therefore, we conclude that

$$f(P) \leq P.$$

□

II.5.7

Find the Sylow 2-subgroups and Sylow 3-subgroups of S_3, S_4, and S_5.

(a) S_3:

- Sylow 2-subgroups: There are three Sylow 2-subgroups, each of order 2. They are generated by the transpositions:

$$\langle(1\ 2)\rangle, \quad \langle(1\ 3)\rangle, \quad \langle(2\ 3)\rangle.$$

- Sylow 3-subgroup: There is one Sylow 3-subgroup, which is of order 3. It is generated by the 3-cycles:

$$\langle(1\ 2\ 3)\rangle.$$

(b) S_4:

- From Proposition II.6.3 we have that there are (up to isomorphism) exactly two distinct nonabelian groups of order 8: D_4 and Q_8. We have that $|S_4| = 24 = 2^3 \cdot 3$, so the Sylow 2-subgroups of S_4 are of order 8. The Sylow 2-subgroups of S_4 are isomorphic to D_4. There are three such Sylow 2-subgroups, which can be described as follows:

$$\langle(1\ 2),(1\ 3)(2\ 4)\rangle, \quad \langle(1\ 3),(1\ 2)(3\ 4)\rangle, \quad \langle(1\ 4),(1\ 2)(3\ 4)\rangle.$$

  These are the only Sylow 2-subgroups of S_4 since any other subgroup of order 8 would have to be isomorphic to Q_8, which cannot be embedded in S_4.

- Sylow 3-subgroup: There are four Sylow 3-subgroups, each of order 3. This is because the number of Sylow 3-subgroups, denoted by n_3, must satisfy the congruence $n_3 \equiv 1 \pmod 3$ and also divide the order of the group. Assuming the group order is such that these conditions are met, we find that $n_3 = 4$ satisfies both requirements. They are generated by the 3-cycles:

$$\langle(1\ 2\ 3)\rangle, \quad \langle(1\ 2\ 4)\rangle, \quad \langle(1\ 3\ 4)\rangle, \quad \langle(2\ 3\ 4)\rangle.$$

  There are only four 3-cycles in S_4, so these are all the Sylow 3-subgroups. There are no other subgroups of order 3 in S_4.

(c) S_5:

- Sylow 2-subgroups: There are fifteen Sylow 2-subgroups, each of order 8 as $|S_5| = 120 = 2^3 \cdot 3 \cdot 5$ and by Sylow's Theorems we have that $15 \equiv 1 \pmod 2$ and $15|120$. They can be generated by various combinations of transpositions and products of disjoint transpositions. For example, one such Sylow 2-subgroup is:

$$\langle(1\ 2),(3\ 4),(1\ 3)(2\ 4)\rangle.$$

  Other Sylow 2-subgroups can be found by considering different sets of transpositions and their products. They are all isomorphic to D_4. There are no Sylow 2-subgroups isomorphic to Q_8 in S_5.

- Sylow 3-subgroups: There are ten Sylow 3-subgroups, each of order 3. This is because the number of Sylow 3-subgroups, denoted by n_3, must satisfy the congruence $n_3 \equiv 1 \pmod 3$ and also divide the order of the group. Assuming the group order is such that these conditions are met, we find that $n_3 = 10$ satisfies both requirements. They are generated by the 3-cycles.

II.5.8

If every Sylow p-group of a finite group G is normal for every prime p, then G is the direct product of its Sylow subgroups.

Proof. Let $|G| = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ be the prime factorization of the order of G, where $p_1, p_2, \ldots, p_m$ are distinct primes and $k_1, k_2, \ldots, k_m$ are positive integers. Let P_i be a Sylow p_i-subgroup of G for each $i = 1, 2, \ldots, m$. By assumption, each P_i is normal in G.

Since each P_i is normal in G, we have that for any $g \in G$ and any $x \in P_i$, the conjugate $gxg^{-1} \in P_i$. This implies that the product of any two elements from different Sylow subgroups commutes. Specifically, for any $x \in P_i$ and $y \in P_j$ with $i \neq j$, we have

$$xy = yx.$$

Now, consider the product of all Sylow subgroups:

$$H = P_1 P_2 \cdots P_m.$$

Since the orders of the Sylow subgroups are relatively prime (i.e., $\gcd(|P_i|, |P_j|) = 1$ for $i \neq j$), it follows that the order of H is given by

$$|H| = |P_1||P_2| \cdots |P_m| = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m} = |G|.$$

Therefore, we have that $H = G$.

To show that G is the direct product of its Sylow subgroups, we need to verify that the intersection of any two distinct Sylow subgroups is trivial. Suppose there exists an element $x \in P_i \cap P_j$ for some $i \neq j$. Then the order of x must divide both $|P_i|$ and $|P_j|$. However, since the orders of these subgroups are powers of distinct primes, the only element that can satisfy this condition is the identity element. Thus, we have

$$P_i \cap P_j = \{e\} \quad \text{for } i \neq j.$$

Therefore, we conclude that

$$G \cong P_1 \times P_2 \times \cdots \times P_m,$$

where $P_1, P_2, \ldots, P_m$ are the Sylow subgroups of G. Hence, G is the direct product of its Sylow subgroups. $\square$

II.5.9

If $|G| = p^n q$ with $p > q$ primes, then G contains a unique normal subgroup of index q.

Proof. Let $|G| = p^n q$ where p and q are distinct primes with $p > q$. By Sylow's theorems, the number of Sylow q-subgroups of G, denoted by n_q, satisfies the following conditions:

1. $n_q \equiv 1 \mod q$
2. n_q divides p^n

Since p^n is a power of the prime p and does not contain the prime factor q, the only divisors of p^n are powers of p. Therefore, the possible values for n_q are limited to powers of p. The smallest power of p is 1, which satisfies both conditions:

$$n_q = 1 \equiv 1 \mod q$$

and

$$1 \text{ divides } p^n.$$

Since $n_q = 1$, there is exactly one Sylow q-subgroup in G. Let this unique Sylow q-subgroup be denoted by Q. Because there is only one such subgroup, it must be normal in G.

The index of this subgroup in G is given by

$$[G : Q] = \frac{|G|}{|Q|} = \frac{p^n q}{q} = p^n.$$

Thus, we have found a unique normal subgroup of index q in G, which is the Sylow q-subgroup Q.

Therefore, we conclude that if $|G| = p^n q$ with $p > q$ primes, then G contains a unique normal subgroup of index q. $\square$

Problem 1

Let G be a group and H_1 and H_2 be two subgroups. Construct bijections between the following sets:

(a) The quotient of G/H_1 by the action of H_2 (on the left).

(b) The quotient of G/H_2 by the action of H_1 (on the left).

(c) The quotient of G by the action of $H_1 \times H_2$ with H_1 action on the left and H_2 acting on the right (i.e., $H_1 \times H_2$ as a subgroup of $G \times G$).

(d) The quotient of $(G/H_1) \times (G/H_2)$ with G acting on two copies simultaneously (this is called the *diagonal action*).

(Going between definitions sometimes requires inverting elements of g.) The resulting set is the *double coset* space $H_1 \backslash G/H_2$; it can be interpreted as the set of *double cosets* $H_1 g H_2$.

Bijection between (a) and (b): Define $\phi_1 : (G/H_1)/H_2 \to (G/H_2)/H_1$ by $\phi_1(H_2(gH_1)) = H_1(gH_2)$. This map is well-defined because if $gH_1 = g'H_1$ for some $g, g' \in G$, then $g' = gh$ for some $h \in H_1$, and thus $H_1(g'H_2) = H_1(ghH_2) = H_1(gH_2)$. Surjectivity follows since for any $H_1(gH_2) \in (G/H_2)/H_1$, we can find a corresponding $H_2(gH_1) \in (G/H_1)/H_2$. Injectivity follows from the fact that if $\phi_1(H_2(gH_1)) = \phi_1(H_2(g'H_1))$, then by the definition of ϕ_1, we have $H_1(gH_2) = H_1(g'H_2)$. This equality implies that the cosets gH_2 and $g'H_2$ are the same, since H_1 is well-defined and respects the equivalence relation. Consequently, $gH_2 = g'H_2$ leads to $gH_1 = g'H_1$, as g and g' must belong to the same coset with respect to H_1. Therefore, ϕ_1 is injective.

Bijection between (b) and (c): Define $\phi_2 : (G/H_2)/H_1 \to G/(H_1 \times H_2)$ by $\phi_2(H_1(gH_2)) = (H_1 \times H_2)(g)$. This map is well-defined because if $gH_2 = g'H_2$ for some $g, g' \in G$, then $g' = gh$ for some $h \in H_2$, and thus $(H_1 \times H_2)(g') = (H_1 \times H_2)(gh) = (H_1 \times H_2)(g)$. Surjectivity follows since for any $(H_1 \times H_2)(g) \in G/(H_1 \times H_2)$, we can find a corresponding $H_1(gH_2) \in (G/H_2)/H_1$. Injectivity follows from the fact that if $\phi_2(H_1(gH_2)) = \phi_2(H_1(g'H_2))$, then $(H_1 \times H_2)(g) = (H_1 \times H_2)(g')$, which implies $g' = h_1 g h_2$ for some $h_1 \in H_1$ and $h_2 \in H_2$, and hence $gH_2 = g'H_2$.

Bijection between (c) and (d): Define $\phi_3 : G/(H_1 \times H_2) \to ((G/H_1) \times (G/H_2))/G$ by $\phi_3((H_1 \times H_2)(g)) = G(gH_1, gH_2)$. This map is well-defined because if $(H_1 \times H_2)(g) = (H_1 \times H_2)(g')$ for some $g, g' \in G$, then $g' = h_1 g h_2$ for some $h_1 \in H_1$ and $h_2 \in H_2$, and thus $G(g'H_1, g'H_2) = G(h_1 g h_2 H_1, h_1 g h_2 H_2) = G(gH_1, gH_2)$. Surjectivity follows since for any $G(gH_1, gH_2) \in ((G/H_1) \times (G/H_2))/G$, we can find a corresponding $(H_1 \times H_2)(g) \in G/(H_1 \times H_2)$. Injectivity follows from the fact that if $\phi_3((H_1 \times H_2)(g)) = \phi_3((H_1 \times H_2)(g'))$, then by the definition of ϕ_3, we have $G(gH_1, gH_2) = G(g'H_1, g'H_2)$. This equality implies that the cosets (gH_1, gH_2) and $(g'H_1, g'H_2)$ are identical under the action of G. Consequently, there exists some $h \in G$ such that $g' = hg$, where h is an element of the group G that relates g and g'. Substituting this back, we see that $(H_1 \times H_2)(g) = (H_1 \times H_2)(g')$, which confirms that ϕ_3 is injective because distinct elements in the domain map to distinct elements in the codomain.

Problem 2

Fix n and put S_n; for any $m \leq n$, let $H_m \subset S_n$ be the subgroup $S_m \times S_{n-m}$. The quotient G/H_m can be identified with the set of m-element subsets of the set $\{1, 2, \ldots, n\}$. (How?) Show that the double quotient $H_{m_1} \backslash G/H_{m_2}$ is a finite set with

$$\min(m_1, m_2) - \max(0, m_1 + m_2 - n) + 1$$

elements. (Hint: the set counts the number of possible relative positions of two subsets of size m_1 and m_2.

Proof. Let $G = S_n$ and consider the subgroups $H_{m_1} = S_{m_1} \times S_{n-m_1}$ and $H_{m_2} = S_{m_2} \times S_{n-m_2}$. The quotient G/H_{m_1} can be identified with the set of m_1-element subsets of $\{1, 2, \ldots, n\}$, and similarly, G/H_{m_2} can be identified with the set of m_2-element subsets of $\{1, 2, \ldots, n\}$.

The double quotient $H_{m_1} \backslash G/H_{m_2}$ represents the set of orbits of the action of H_{m_1} on the left cosets of H_{m_2} in G. Each orbit corresponds to a distinct way of positioning an m_1-element subset relative to an m_2-element subset within the n-element set.

To determine the number of distinct relative positions, we analyze how many elements can be shared between the two subsets. Let k denote the number of elements common to both subsets. The value of k is constrained by the following:

Suppose A and B are m_1-element and m_2-element subsets, respectively. The intersection $A \cap B$ can have at most $\min(|A|, |B|) = \min(m_1, m_2)$ elements, since the intersection cannot exceed the size of the smaller subset.

Similarly, if $m_1 + m_2 \leq n$, the subsets can be disjoint, so the minimum overlap is $k = 0$. If $m_1 + m_2 > n$, the subsets must share at least $m_1 + m_2 - n$ elements, because there are only n elements in total, and the subsets together contain $m_1 + m_2$ elements.

Thus we have that the double quotient $H_{m_1} \backslash G/H_{m_2}$ has exactly $\min(m_1, m_2) - \max(0, m_1 + m_2 - n) + 1$ elements, corresponding to the possible values of k. $\square$

Problem 3

(A follow-up to II.5.9) Suppose G is a finite group, and that p is the smallest prime factor of $|G|$. Show that any subgroup $H \subset G$ of index p is normal.(One possible way to prove this: consider the action of H on G/H, and notice that the trivial coset H is a fixed point.)

Proof. Let S be the set of all left cosets of H in G. Since $[G : H] = p$, the group G acts on S by left multiplication, and this action induces a homomorphism $\phi : G \to A(S)$, where $A(S)$ is the group of permutations of S. Since $|S| = p$, we have $A(S) \cong S_p$, the symmetric group on p elements.

Let $K = \ker(\phi)$ be the kernel of this homomorphism. By the First Isomorphism Theorem, $G/K \cong \mathrm{im}(\phi)$, which is a subgroup of $A(S) \cong S_p$. Hence, $|G/K|$ divides $|S_p| = p!$. Furthermore, since $K = \ker(\phi)$, it is a normal subgroup of G, and $K \subseteq H$ because H is the stabilizer of the trivial coset H under the action of G on S.

Now, since $|G| = pm$, we know that p is the smallest prime factor of $|G|$. This implies that $p!$ cannot divide m, because $p!$ contains factors larger than p that are not divisors of $|G|$. Therefore, the only divisors of $|G/K| = [G : K]$ that are consistent with $|G| = |K|[G : K]$ are 1 and p.

Since $[G : K] = |G/K| \geq p$, it follows that $|G/K| = p$. Thus, $[H : K] = \frac{|H|}{|K|} = 1$, which implies that $H = K$. Since K is normal in G, we conclude that H is normal in G. $\square$