Notes on the Proof of the Sylow Theorems

1 The Theorems

We recall a result we saw two weeks ago.

Theorem 1.1 ***Cauchy's Theorem for Abelian Groups*** *Let A be a finite abelian group. If p is a prime number that divides its order, then A must have an element of order p.*

Theorem 1.2 ***Sylow's First Theorem*** *Let G be a finite group. Let p be a prime number such that its power by α is the largest power that will divide $|G|$. Then there exists at least one subgroup of order p^α. Such subgroups are called Sylow p-subgroups.*

Proof We divide the proof into two cases.
Case One: p divides the order of the center $Z(G)$ of G. By Cauchy's Theorem for abelian groups, $Z(G)$ must have an element of order p, say a. By induction, the quotient group $G/ < a >$ must have a subgroup P_0 of order $p^{\alpha-1}$. Then the pre-image of P_0 in $Z(G)$ is the desired subgroup of order p^α. (Note: in general, if S is any subset of a quotient group G/H, then the order of the pre-image of S is the product of its order with the order of the subgroup.)
Case Two: assume that p does not divide the order of the center of G. Write $|G|$ in terms of the "class equation:"

$$|G| = |Z(G)| + \sum |\text{Conj}(a)|,$$

where the sum is over all the distinct non-central conjugacy classes of G; that is, conjugacy class with more than one element. Since p fails to divide the order of the center, there must be at least one non-central conjugacy class, say $\text{Conj}(b)$, whose order is not divisible by p. Recall that $|\text{Conj}(b)| = [G : C_G(b)] = |G|/|C_G(b)|$. We observe immediately that p^α must divide the order of the subgroup $C_G(b)$. Again, by induction, G will have a Sylow p-subgroup. This ends the proof.

Corollary 1.1 *There is a subgroup Q of a Sylow p-subgroup P for every power of p that divides the order of the group G.*

Corollary 1.2 *If every element of a group is a power of a prime p, then the group is a p-group; that is, the order of the group is a power of p.*

Theorem 1.3 ***Sylow's Second Theorem*** *Let n_p be the number of Sylow p-subgroups of a finite group G. Then $n_p \equiv 1 \bmod p$.*

Proof We begin with a claim.
Claim: Let P be any Sylow p-subgroup. If $g \in G$ be a p-element and $gPg^{-1} = P$, then $g \in P$. To see this, consider the subgroup R generated by g and P. By assumption, $g \in N_G(P)$, so $R \leq N_G(P)$. Hence, P is a normal subgroup of R. We find $|R| = |R/P| \cdot |P|$. But $|R/P|$ is a cyclic group generated by the coset gP. Then gP is a p-element since g is. Hence $|R|$ is a power of p since all its elements are p-elements.
Let $\mathcal{S}_p$ be the set of all Sylow p-subgroups of G. Then G acts on this set by conjugation. Let $P, Q \in \mathcal{S}_p$ be two distinct subgroups. Then Q cannot be fixed under conjugation by all the elements of P because of the Claim.

Let $\mathcal{O}$ be the P-orbit of Q under conjugation. Then the size of the orbit must be divisible by p because of the order-stabilizer equation:

$$|\mathcal{O}| = \frac{|P|}{|\mathrm{Stab}_P(Q)|}.$$

Since $|P|$ is a power of p, the size of any orbit must be a power of p. The case $|\mathcal{O}| = p^0 = 1$ is ruled out since Q cannot be fixed by all the elements of P.
We find that the set of all Sylow p-subgroups is the union of P-orbits. There is only one orbit of order one, $\{P\}$, while the other orbits must have orders a positive power of p.
We conclude $n_p = |\mathcal{S}_p| \equiv 1 \bmod p$.

Remark: We want to emphasize a result from this proof. Let P be any Sylow p-subgroup. As above, we let P act on $\mathcal{S}_p$ by conjugation. Let S_0 be any P-invariant subset of $\mathcal{S}_p$, which means that is a disjoint union of P-orbits. Then $|S_0| \equiv 0 \bmod p$ if $P \notin S_0$; while $|S_0| \equiv 1 \bmod p$ if $P \in S_0$.

Theorem 1.4 *Any two Sylow p-subgroups are conjugate.*

PROOF Let P be any Sylow p-subgroup. Let S_0 be the set of all G-conjugates of P. Then S_0 is P-invariant and $P \in S_0$. By the above observation, $|S_0| \equiv 1 \bmod p$. If S_0 does not exhaust the set of all Sylow p-subgroups, choose one, say Q, not in S_0. Let S_1 be the set of all G-conjugates of Q. By the same reasoning as for S_0 with Q playing the role of P, we must have $|S_1| \equiv 1 \bmod p$. On the other hand, S_1 is P-invariant and $P \notin S_1$. By the above observation, $|S_1| \equiv 0 \bmod p$. Contradiction.

Corollary 1.3 *The number n_p of Sylow p-subgroups must divide $|G|/p^\alpha$.*

PROOF Recall that the number of conjugates of any subgroup H in a group G is given by

$$\#\text{conjugates} = \frac{|G|}{|N_G(H)|}$$

If H is a Sylow p-subgroup, then the order of its normalizer must be divisible by p^α since $H \leq N_G(H)$. But the number of all Sylow p-subgroups is just the number of conjugates of any one of them.

Theorem 1.5 *Any p-subgroup B is contained in a Sylow p-subgroup.*

PROOF Let B act on the space $\mathcal{S}_p$ by conjugation. Then the size of any B-orbit $\mathcal{O}$ must be a power of p, since the $|\mathcal{O}| = [G : N_G(B)]$. Since the size of $\mathcal{S}_p$ is not a power of p, there must be at least one B-orbit with one element, say P. But B must be a subgroup of P since the subgroup generated by B and P is a power of p, by the corollary to Sylow's First Theorem.

Theorem 1.6 *Any finite abelian group is a product of its Sylow p-subgroups.*

As a consequence of this last theorem, to classify the finite abelian groups, it is enough to understand their structure in the case that their order of a power of a prime. One can show that if $|A| = p^n$, then A is isomorphic to a group of the form $\mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times \cdot \mathbf{Z}_{n_k}$, where $n_1 \geq n_2 \geq \cdots \geq n_k$ and $n_1 + \cdots n_k = n$.

2 Other Theorems

I close with the statement of three theorems of Burnside. Their proofs is beyond the scope of the course.

Theorem 2.1 *Let P be a Sylow p-subgroup of a finite group G. If P is central in its own normalizer, then G has a normal subgroup U such that $G = P \cdot U$ and $P \cap U = \{e\}$.*

Theorem 2.2 *Let G be a finite group of order N in which every Sylow subgroup is cyclic. Then G is generated by two elements A and B with the relations:*

$$\begin{aligned} A^m = B^n = 1, BAB &= A^r, N = mn \\ \mathrm{GCD}((r-1)n, m) = 1, r^n &\equiv 1 \bmod m. \end{aligned}$$

Theorem 2.3 *If a finite group G has a conjugacy class whose size is p^k, where p is a prime and $k \geq 1$, then G cannot be a simple group.*

3 Semi-Direct Products

Suppose $G = A \cdot Q$ where A is normal in G. Then we can work with G as ordered pairs:

$$(a_1 q_1) \cdot (a_2 q_2) = a_1(q_1 a_2)q_2 = a_1(q_1 a_2 q_1^{-1})q_1 q_2.$$

So, we can define the multiplication on ordered pairs as:

$$(a_1, q_1) \cdot (a_2, q_2) = (a_1 \alpha(q_1)(a_2), q_1 q_2),$$

where $\alpha(q)(x) = qxq^{-1}$.
The inverse of (a, q) is given by $(\alpha(q^{-1})a^{-1}, q^{-1})$.
Note that we can treat α as a homorphism from the group Q into the automorphism of A.
In fact, this is all we need to define such a group G: we are given two groups A and Q and a homomorphism from Q into $\mathrm{Aut}(A)$. The resulting group is called the *semidirect product* of Q with A. As a consequence, it is now important to understand the automorphism groups of some low order abelian groups because it is through them that many non-abelian groups may be constructed.
It is useful to verify that $\{(a, 1_Q) : a \in A\}$ is a normal subgroup of the semidirect product isomorphic to A while $\{(1_A, q) : q \in Q\}$ is a subgroup of the semidirect product isomorphic to Q. Furthermore, we can verify that

$$(1_A, q)(a, 1_Q)(1_A, q)^{-1} = (\alpha(q)a, 1_Q).$$

We give a brief review of some automorphism groups of some abelian groups. For $\mathbf{Z}_p$, where p is a prime, then $\mathrm{Aut}(\mathbf{Z}_p) \cong \mathbf{Z}_p^{\times}$; that is the group of positive integers less than p under multiplication modulo p. For $\mathbf{Z}_m$, where m is composite, then $\mathrm{Aut}(\mathbf{Z}_m) \cong U(\mathbf{Z}_m)$; that is, the group of positive integers less than m and relatively prime to m under multiplication modulo m. For example, $\mathrm{Aut}(\mathbf{Z}_4)$ is $\{1, 3\}$ and is isomorphic to $\mathbf{Z}_2$; while $\mathrm{Aut}(\mathbf{Z}_6)$ is $\{1, 5\}$ and is also isomorphic to $\mathbf{Z}_2$. For $G = \mathbf{Z}_p \times \mathbf{Z}_p$, where p is prime, we find that $\mathrm{Aut}(G) \cong \mathrm{GL}(2, \mathbf{Z}_p)$.
Note: one way to give a homomorphism of a cyclic group $\mathbf{Z}_n$ into any of the above automorphism groups is to find an explicit automorphism of order n in the automorphism group itself. Further, in

forming such as homomorphism we also note the basic fact that if $\phi : G_1 \to G_2$ is any homomorphism between two groups and $x \in G_1$ then the order $\phi(x) \in G_2$ must divide $|G_2|$ as well as $|x|$. Hence, the order of $\phi(x)$ must be a *common divisor* of $|G_1|$ and $|G_2|$.

Examples:

1. The dihedral groups D_n are all semidirect products where $A = \mathbf{Z}_n$ and $Q = \mathbf{Z}_2 = \{0, 1\}$ with the map $\alpha(q)(x) = (-1)^q x$, where $x = 0$ or 1. (We may also write $\alpha(1)(x) = (n-1) \cdot x$.

   Let x be a generator of $A = \mathbf{Z}_n$ and write $a = (x, 0)$ and $b = (0, 1)$. We find:

   $$\begin{aligned} ab &= (x,0) \cdot (0,1) = (x + \alpha(1) \cdot 0, 0_1) = (x, 1) \\ ba &= (0,1) \cdot (x,0) = (0 + \alpha(1) \cdot x, 1 + 0) = (-x, 0). \end{aligned}$$

   In particular, a and b satisfy the relations for the dihedral group: $a^n = e, b^2 = e$, and $ab = ba^{-1}$.

2. Since $\mathrm{Aut}(\mathbf{Z}_n)$ is isomorphic to $U(n)$, we may readily generalize this example.

3. Let $A = \mathbf{Z}_2 \times \mathbf{Z}_2$ and $Q = S_3$. Note: $\mathrm{Aut}(\mathbf{Z}_2 \times \mathbf{Z}_2) \cong S_3$. The resulting group has order of 24.

4. Let F be a field then we can form the semidirect product of F with F^* with $\alpha(f)\, x = f \cdot x$ where $f \in F^*$ and $x \in F$:

   $$(f_1, x_1) \cdot (f_2, x_2) = (f_1 + \alpha(x_1) f_2, x_1 x_2).$$

5. Consider the semidirect product of F^n with $\mathrm{GL}(n, F)$ by:

   $$(f_1, T_1) \cdot (f_2, T_2) = (f_1 + T_1 f_1, T_1 T_2).$$

   Note with $n = 2$ and $F = \mathbf{Z}_2$, we obtain another group of order 24.

6. We can construct a group G of order 20 by a semidirect product of $\mathbf{Z}_5$ with $\mathbf{Z}_4$ because $\mathrm{Aut}(Z_5) \cong \mathbf{Z}_4$:

   $$(a_1, b_1) \cdot (a_2, b_2) = (a_1 + \alpha(b_1) a_2, b_1 + b_2).$$

   Note: G has generators x and y satisfying $x^5 = y^4 = e$ and $xyx = y$. This example is a special case of the procedure in (4) with $F = \mathbf{Z}_5$.

   Another realization of this group is the subgroup of S_5 generated by the two cycles $\rho = (1, 2, 3, 4, 5)$ with $\sigma = (2, 3, 5, 4)$ so that the conjugate of ρ by σ is a power of ρ.

7. One can show that the group of order eight of unit quaternions cannot be expressed as a semidirect product.

8. Examples (4) and (6) are particular instances of a *metacyclic* group which is given as the semidirect product of $\mathbf{Z}_n$ with its automorphism group $U(n)$. Note that the metacyclic group can be viewed as a subgroup of the symmetric group S_n. We will see this group later in our study of Galois theory in connection with the roots of $x^n - 2 = 0$.

9. There is a canonical semidirect product associated to any group G. Let $n > 0$. Let $S(n)$ act on the product group $G^n = G \times G \times \cdots \times G$ (n-times) by permuting coordinates, that is, if $\sigma \in S(n)$, let $\sigma \cdot (x_1, x_2, \ldots, x_n) = (x_{s(1)}, (x_{\sigma(2)}, \ldots, x_\sigma(n))$. The resulting semidirect product group is called the *wreath product* of S_n with G. It has order $n!\,|G|^n$. The group of *signed* permutation matrices and the symmetry group of the cube are examples of wreath products.

10. The group G of signed $n \times n$ matrices can be expressed as a semidirect product of the normal subgroup of all diagonal matrices $\mathrm{diag}(\pm 1, \pm 1, \ldots, \pm 1)$ where the signs are chosen independently and the subgroup of all permutation matrices. The normal subgroup of G consisting of all matrices of determinant 1 gives the group of rotations of the cube in n-space. It is a group of order $2^{n-1}n!$. This is another natural family of non-abelian groups.

4 Sylow Theory and Classification of Low Order Groups

We begin by stating some basic results about the normality of Sylow p-subgroups. These statements all follow easily from the techniques described introducted the last lecture. Below we shall refine these techniques to give an actual classification of all groups of a given order.

1. If $|G| = pq$ where $p < q$ are distinct primes, then
   (a) if $p \not| (q-1)$, then there are unique Sylow p and q subgroups.
   (b) if $p \,|\, (q-1)$, then there is a unique Sylow q subgroup only.
2. If $|G| = pqr$ where $p < q < r$ are distinct primes, then
   (a) the Sylow r-subgroup is normal.
   (b) G has a normal subgroup of order qr.
   (c) if $q \not| (r-1)$, then the Sylow q-subgroup of G is normal.
3. If $|G| = p^2q$ where p and q are primes, then either the Sylow p or Sylow q subgroups are normal.

It is useful to experiment with integers that have the above the prime factorizations.

5 Classification of Groups 12

We will move onto the classification of groups of order 12. The groups we know are: two abelian: $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3$, $\mathbf{Z}_4 \times \mathbf{Z}_3$, and two non-abelian: the alternating group A_4 and the dihedral group $D_6 \cong S_3 \times \mathbf{Z}_2$.
Further, last week we characterized A_4 among the groups of order 12 as having $n_3 = 4$. In fact, we saw that if G is any group of order 12 with $n_3 = 4$, then there was a homomorphism of G into the group of permutations of the set of the four Sylow 3-subgroups. By considering the elements of order 3 and counting, we found that the image of G in S_4 was contained in A_4. Since they have the same order, they must be equal.

It is now easy to classify the abelian groups A of order 12. By Sylow theory, we know that A has two unique subgroups P_3 of order 3 and P_2 of order 4. By the recognition of direct products theorem, we find $A \cong P_3 \times P_2$. Recall that we have already classified the abelian subgroups of order 3 and 4. They are for order 3: $\mathbf{Z}_3$ while for order 4: $\mathbf{Z}_4$ or $\mathbf{Z}_2 \times \mathbf{Z}_2$. Note: $\mathbf{Z}_{12} \cong \mathbf{Z}_4 \times \mathbf{Z}_3$.
It remains to examine the case $n_3 = 1$ for a non-abelian group of order 12. Let P_3 be the unique Sylow 3-subgroup, which must be normal. Let P_2 be some Sylow 2-subgroup. Then $G = P_3 \cdot P_2$; that is, G must be a semidirect product of P_2 with the cyclic group of order 3: $\mathbf{Z}_3$. Further, $\mathrm{Aut}(\mathbf{Z}_3) \cong \mathbf{Z}_3^{\times}$, that is, it is isomorphic to $\{1, 2\}$ under multiplication modulo 3. So, there is a only one non-trivial automorphism, say α, of order 2 given by $x \mapsto 2x$, for $x \in \mathbf{Z}_3$.
There are two main cases.

1. For the first case, $P_2 \cong \mathbf{Z}_2 \times \mathbf{Z}_2$. We need to consider homomorphisms θ from P_2 into the automorphism group of $\mathbf{Z}_3$, which itself is isomorphic to $\mathbf{Z}_2$. There are three non-trivial homomorphisms θ_i, $i = 1, 2, 3$. To construct them, let a, b, c be the non-identity elements of P_2. We find: $\theta_1(a) = \alpha$, while $\theta_1(b) = \theta_1(c) = \mathrm{Id}$; $\theta_2(b) = \alpha$, while $\theta_2(a) = \theta_2(c) = \mathrm{Id}$; $\theta_3(c) = \alpha$, while $\theta_3(a) = \theta_3(b) = \mathrm{Id}$. The resulting semidirect product group is isomorphic to $D_6 \cong S_3 \times \mathbf{Z}_2$.

2. For the second remaining case, $P_2 \cong \mathbf{Z}_4$. Then for a non-trivial homomorphism θ must map the generator 1 of $(\mathbf{Z}_4, +)$ onto the α. The resulting non-abelian group is not isomorphic to the ones consider already.

To conclude, there are three non-abelian groups of order 12 and two abelian ones.

6 Classification of Groups of Order 30

Let G be a group of order $30 = 2 \cdot 3 \cdot 5$, the product of three distinct primes.
Let n_p denote the number of distinct Sylow p-subgroups of G. Then we know that $n_p \equiv 1 \bmod p$ and n_p must divide $|G|/p^e$, where p^e is the maximal power of p that divides $|G|$.
In our case, we find that $n_3 = 1 + 3k$ and must divide 10 so $n_3 = 1$ or 10 while $n_5 = 1 \mod 5$ and n_5 must divide 6 so $n_5 = 1 or 6$.
Now, either n_3 or n_5 must equal 1; for otherwise, G would contain 20 elements of order 3 and 24 elements of order 5.
Let P_3 be a Sylow 3-subgroup and P_5 be a Sylow 5-subgroup. We know that one of them must be a normal subgroup. As a consequence, the product set H $P_3 \cdot P_5$ is, in fact, a subgroup of G of order 15.
Because the index $[G : H] = 2$, we find that H is a normal subgroup of G. Further, by our comments last time about the structure of groups whose orders are the product of two distinct primes, we know that $H \cong \mathbf{Z}_3 \times \mathbf{Z}_5$ since $3 \not| (5 - 1) = 4$.
Since H is normal in G, $G = H \cdot P_2$ where P_2 is some Sylow 2-subgroup of order 2.
To sum up, to determine the structure of groups of order 30, we only determine the number of possible semidirect products of $\mathbf{Z}_3 \times \mathbf{Z}_5$ with $\mathbf{Z}_2$.
Let $\theta : \mathbf{Z}_2 \to \mathrm{Aut}(\mathbf{Z}_3 \times \mathbf{Z}_5)$.
We may easily verify that

$$\mathrm{Aut}(\mathbf{Z}_3 \times \mathbf{Z}_5) \cong \mathrm{Aut}(\mathbf{Z}_3) \times \mathrm{Aut}(\mathbf{Z}_5)$$

since $\mathbf{Z}_3$ and $\mathbf{Z}_5$ are simple groups of distinct orders.
In particular, θ becomes a homomorphism from $\mathbf{Z}_2$ to $U(\mathbf{Z}_3) \times U(\mathbf{Z}_5)$ or $\mathbf{Z}_2 \to \mathbf{Z}_2 \times \mathbf{Z}_4$.
Let a be a generator of $U(\mathbf{Z}_3) \cong \mathbf{Z}_2$, b a generator for $U(\mathbf{Z}_5) \cong \mathbf{Z}_4$ while c a generator for $\mathbf{Z}_2$.
Then there are exactly four choices for θ; they are:

$$\begin{array}{cccc} a \to a, & a \to a, & a \to a^{-1}, & a \to a^{-1} \\ b \to b, & b \to b^{-1}, & b \to b, & b \to b^{-1} \end{array}$$

We find that the resulting semidirect product groups are all non-isomorphic by considering their centers. The order of the centers from left to right are $30, 3$ (generated by a), 5 (generated by b), and 1. Of course, if the center has order 30, then the group is abelian.

7 Classification of Groups of Order 28

Let G be a group of order $28 = 4 \cdot 7 = 2^2 \cdot 7$. Let n_p denote the number of Sylow p-subgroups as usual. Then $n_7 \equiv 1 \mod 7$ and n_7 must divide 4. Hence $n_7 = 1$ and the only Sylow 7-subgroup P_7 is normal and isomorphic to $\mathbf{Z}_7$.
Let P_2 be a Sylow 2-subgroup of order 4. Then P_2 may be isomorphic to either group of order 4: $\mathbf{Z}_4$ or $\mathbf{Z}_2 \times \mathbf{Z}_2$.
Since P_7 is normal in G, the group $G = P \cdot P_2$; that is, a semidirect product of P_7 with P_2.
Hence, we need to classify these semidirect products or equivalently the homomorphisms θ from P_2 into $\mathrm{Aut}(P_7)$, in particular,

$$\theta : \mathbf{Z}_4 \to U(Z_7)$$
$$\theta : \mathbf{Z}_2 \times \mathbf{Z}_2 \to U(\mathbf{Z}_7)$$

where $\mathrm{Aut}(\mathbf{Z}_7) \cong U(\mathbf{Z}_7)$, the multiplicative group of integers relatively prime to 7. Note: $U(7) \cong \mathbf{Z}_6$.

1. We first study the case that the Sylow 2-subgroup is cyclic to isomorphic to $\mathbf{Z}_4$. Write $\mathbf{Z}_4 =< a >$ and $b = \theta(a) \in U(7)$. Then $|b|$ is a common divisor of 4 and 6. The only choices for its order are 1 and 2.

   If $|b| = 1$, G is simply the direct product of $\mathbf{Z}_4$ and $\mathbf{Z}_7$.

   When $|b| = 2$, we need to find the elements of order 2 in $U(7) = \{1, 2, 3, 4, 5, 6\}$ under multiplication modulo 7. There is only one such element: 6. Hence, there is exactly one such homomorphism $\theta : \mathbf{Z}_4 \to U(7)$ given by $\theta(x) = 6x \in U(7)$.

2. If the Sylow 2-subgroup is isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_2$, then the needed homomorphism has the form:

   $$\theta : \mathbf{Z}_2 \times \mathbf{Z}_2 \to U(7)$$

   As in the last case, the trivial homomorphism yields the direct product group $\mathbf{Z}_2 \times \mathbf{Z}_2 \times Z_7$. For θ to be non-trivial, we determine its actions on the generators $a_1 = (1, 0), a_2 = (0, 1)$ and $a_3 = (1, 1)$ in $\mathbf{Z}_2 \times \mathbf{Z}_2$. Now, exactly two of the three generators may map to 6 while the third maps to 1. However, each such choice for θ gives an isomorphic group.

We conclude that there are four groups of order 28 of which 2 are abelian and 2 are non-abelian.

8 Comments on Groups of Order 60

Let G be a group of order $60 = 2^2 \cdot 3 \cdot 5$. Then G has Sylow p-subgroups of order $4, 3$ and 5. We can show that there are 13 distinct isomorphism types of groups of order 60.

8.1 G is simple

Assume G is a simple group of order 60. Then $n_5 = 6$ and $n_3 = 10$. By simplicity, $n_3 > 1$ and $n_5 > 1$. Now, $n_5 \equiv 1 \bmod 5$ and $n_5|12$ which implies n_5 must equal 6. For n_3, we similarly find $n_3 \equiv 1 \bmod 3$ and $n_3|20$. Hence, n_3 equals either 4 or 10. Suppose $n_3 = 4$ so there are 4 Syow 3-subgroups forming the set $\mathcal{S}_3$. Then G acts transitively on $\mathcal{S}_3$ which gives a non-trivial homomorphism α from G into S_4. Since G is simple, α must be 1-1. This is impossible since $24 = |S_4| < |G| = 60$. Hence n_3 must equal 10.
Claim I: if G has a subgroup of order 12, then $G \cong A_5$.
To verify the claim, consider the G-action on the coset space G/H. This action gives a non-trivial homomorphism β from G into S_5. Since G is simple, β must be 1-1. Since A_5 is a normal subgroup in S_5, we find $A_5 \cap \beta[G]$ must be a normal subgroup in A_5. Since A_5 is simple, $\beta[G]$ must equal A_5 itself. Hence, the Claim is established.
Claim II: G has a subgroup of order 12.
By simplicity, $n_2 > 1$. By Sylow theory, $n_2 \equiv 1 \bmod 2$ and $n_2|15$ which implies n_2 must equal 5 or 15.
If $n_2 = 5$, then we may let G act on the set $\mathcal{S}_2$ of Sylow 2-subgroups. This gives a non-trivial homomorphism γ from G into S_5. By simplicity, this map is 1-1. Arguing as in Claim I, we find $G \cong A_5$.
If $n_2 = 15$, there must be two Sylow 2-subgroups, say P and Q, with an intersection of order 2. To see this, suppose all 15 Sylow 2-subgroups intersect only at the identity. This gives 45 elements of even order. However G has 24 elements of order 5 and 20 elements of order 3 since $n_5 = 6$ and $n_3 = 10$. This is impossible so there are such subgroups P and Q. Let x be a non-identity element from $P \cap Q$. Of course, x cannot be a generator for either P or Q so it has order 2.
Consider the centralizer $C_G(x)$. Clearly, both P and Q must lie in the centralizer of x. So 4 must be a divisor of the order of $C_G(x)$. Furthermore, by examining the elements of P and Q we find $C_G(x)$ must contain at least six distinct elements as well. Hence $|C_G(x)$ is a common multiple of 4 and 6 and be a divisor of 60 as well. There is only one such integer, namely 12.
Note: one can show that if $n_5 > 1$, then G is automatically simple.

8.2 Sylow 3 and 5 subgroups are normal

We shall assume that the Sylow 3-subgroups P_3 and 5-subgroups P_5 are unique and normal. Then $N = P_3 \cdot P_5$ is a subgroup of G. Further N is a normal subgroup since $gNg^{-1} = gP_3g^{-1}\, gP_5g^{-1} = P_3 \cdot P_5$ for any $g \in G$. Of course, $N \cong \mathbf{Z}_{15}$ and $\mathrm{Aut}(\mathbf{Z}_{15}) = U(\mathbf{Z}_{15})$ which is isomorphic to the set $\{1, 2, 4, 7, 8, 11, 13, 14\}$ under multiplication modulo 15. So $U(\mathbf{Z}_{15}) \cong \mathbf{Z}_4 \times \mathbf{Z}_2$. To sum up, $G = N \cdot H$ where H is a subgroup of order 4. We find *eleven* isomorphism types.

1. $H \cong \mathbf{Z}_4$: We list five distinct homomorphisms θ from $\mathbf{Z}_4$ into $\mathbf{Z}_4 \times \mathbf{Z}_2$.
   (a) $\theta(1) = (0, 0)$.

(b) $\theta(1) = (1, 0)$ or $\theta(1) = (3, 0)$.

(c) $\theta(1) = (2, 0)$.

(d) $\theta(1) = (0, 1)$.

(e) $\theta(1) = (1, 1)$.

2. $H \cong \mathbf{Z}_2 \times \mathbf{Z}_2$: We list six distinct homomorphisms θ from $\mathbf{Z}_2 \times \mathbf{Z}_2$ into $\mathbf{Z}_4 \times \mathbf{Z}_2$.

(a) $\theta(1, 0) = (0, 0)$ and $\theta(0, 1) = (0, 0)$.

(b) $\theta(1, 0) = (2, 0)$ and $\theta(0, 1) = (0, 0)$.

(c) $\theta(1, 0) = (0, 1)$ and $\theta(0, 1) = (0, 0)$.

(d) $\theta(1, 0) = (2, 0)$ and $\theta(0, 1) = (2, 1)$.

(e) $\theta(1, 0) = (0, 1)$ and $\theta(0, 1) = (2, 1)$.

(f) $\theta(1, 0) = (2, 1)$ and $\theta(0, 1) = (0, 0)$.

9 Comments on the Simple Group of Order 168

Recall that the general linear group GL(2, q) over a field with q elements has order $(q^2-1)(q^2-q)$. Its normal subgroup, the special linear group SL(2, q), has order $q(q+1)(q-1)$ since $\det : \mathrm{GL}(2, \mathrm{q}) \to \mathrm{F}^{\times}$ with kernel precisely SL(2, q). Finally, the center of SL(2, q) is $\{\pm I\}$. The resulting quotient group, the projective linear group, PSL(2, q) has order $q(q+1)(q-1)/2$.
We are going to work with the case $q = 7$. Then SL(2, 7) has order 336 and PSL(2, 7) has order 168. A convenient feature of the field of order 7, $\mathbf{Z}_7$, is that its quadratic extension can be realized as the $\mathbf{Z}_7[i]$, that is, the ring (of Gaussian integers) $\mathbf{Z}[i] = \{m + in : m, n \in \mathbf{Z}\}$ with usual complex addition and multiplication considered modulo 7.
We will find the order of each conjugacy class in SL(2, 7) to begin. We present the table of results then give comments.

Conjugacy Classes for SL(2, 7)

Matrix	**Spectral Data**	**Order**	| Conjugacy Class |
I	1,1	1	1
$-I$	1,1	1	1
$D = \mathrm{diag}(3,5)$	3,5	6	56
$-D = \mathrm{diag}(3,5)$	$-3,-5$	3	56
$J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$	$i,-i$	2	42
$J_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$	1	7	24
$-J_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$	-1	7	24
$5(I+J)$	$5(1 \pm i)$	8	42
$-5(I+J)$	$-5(1 \pm i)$	8	42
$J_2 = \begin{bmatrix} 6 & 1 \\ 0 & 6 \end{bmatrix}$	6	14	24
$-J_2 = \begin{bmatrix} 1 & 6 \\ 0 & 1 \end{bmatrix}$	1	14	24

In order to compute the size of a conjugacy class of an element x, it is enough to find the order of the centralizer of x: $\{g \in G : gx = xg\}$. The table entries are arranged to minimize the number of such calculations. It is plain to observe that $\pm I$, $\pm D$ have the same centralizers. Further J and $\pm 5(I+J)$ have the same centralizers as well as the four elements $\pm J_1$ and $\pm J_2$. To find the centralizer of a matrix x, we consider $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and write $gx = xg$. A linear system for the entries a, b, c, d results. A further restriction needs to be applied: $\det(g) = 1$.

It is interesting to note that while J_1 and $-J_2$ have the same spectral data: 1 is the only eigenvalue with multiplicity 1 so are conjugate in the full linear group, they are *not* conjugate in the special linear group.

We next consider how the conjugacy classes in $\mathrm{SL}(2,7)$ relate to those of $\mathrm{PSL}(2,7) = \mathrm{SL}(2,7)/\{\pm \mathrm{I}\}$. We begin with noticing that $g \in C_G(a) \iff -g \in C_G(a)$ where $C_G(a)$ is the centralizer of a in the group $G = \mathrm{SL}(2,7)$. In particular, the size of the set $C_G(a)$ is halved when sent to its image in the quotient group.

On the other hand, a and $-a$ have the same image in the quotient. Hence, the images of the following pairs agree: $\pm I, \pm D, \pm J_1, \pm J_2$, and $\pm 5(I+J)$. Hence, the 11 conjugacy class of $\mathrm{SL}(2,7)$ collapse to 6. If $\pi : \mathrm{SL}(2,7) \to \mathrm{PSL}(2,7)$ be the canonical projection, then $|C_{PSL}(\pi(a))| = |C_{SL}(a)|/2 + |C_{SL}(-a)|/2$, where $a \in \{\pm I, \pm D, \pm J_1, \pm J_2, \pm 5(I+J)$; that is, $a \neq J$.

With these remarks, we have the following table for $\mathrm{PSL}(2,7)$. We use the notation $[a]$ to denote the class of an element of a in the quotient.

Conjugacy Classes for $\mathrm{PSL}(2,7)$

Matrix	**Order**	|ConjugacyClass|
$[I]$	1	1
$[D]$	3	56
$[J]$	2	21
$[J_1]$	7	24
$[5(I+J)]$	4	42
$[J_2]$	7	24

The order of the elements $[x]$ in the above table follow from observing $D^3 = -I$, $J_1^7 = J_2^7 = -I$, and $(5(I+J))^4 = -I$.
We are now able to show that $\mathrm{PSL}(2,7)$ is simple by the same elementary counting argument that we had used for the alternating group A_5.
Let N be a normal subgroup of $\mathrm{PSL}(2,7)$. Then if $a \in N$ so must its entire conjugacy class. That forces the order of N to have the form:

$$|N| = 1 + 56a + 21b + 24c + 42d + 24e,$$

where a, b, c, d, e may equal either 0 or 1. Recall the basic fact that $|N|$ must be a divisor of 168. By case-by-case analysis, we find that there are no solutions for a, b, c, d, e that satisfy these two conditions other than $|N| = 1, 168$. To verify this, it is convenient to separate out the two cases that $|N|$ is odd or even. We conclude that $\mathrm{PSL}(2,7)$ is simple.
We close by counting the Sylow p-subgroups of $\mathrm{PSL}(2,7)$. Note $168 = 2^3 \cdot 3 \cdot 7$. Further, we recall that $n_p = [\mathrm{PSL}(2,7) : N_G(P_p)]$, where P_p is the Sylow p-subgroup.

Sylow p-subgroups P for $G = \mathrm{PSL}(2,7)$

Prime p	**Number** n_p	$\lvert N_G(P)\rvert$
2	21	8
3	28	6
7	8	21

The number of Sylow subgroups for primes 3 and 7 follow immediately from counting the elements of those orders in the group itself. The count for the Sylow 2-subgroups, though, requires a special calculation that requires some work.
If n_p is the number of Sylow p-subgroups, then we find

$$n_p \equiv 1 \bmod p, \quad n_p \,|\, 168$$

as predicted by the Sylow theory.
One can show that P_2 is isomorphic to the dihedral group D_4 of order 8, $N_G(P_3)$ is isomorphic to S_3, and $N_G(P_7)$ has order 21. To verify the results for $p = 3, 7$, observe that $\mathrm{PSL}(2,7)$ has no elements of order 6 nor 21. Hence, the corresponding normalizers cannot be abelian by the classification of groups of order 6 and 21.

10 Detailed Information for Some Low Order Groups

10.1 Symmetric Group S_4

Conjugacy Class	# Elements	Order
$[4]$	6	4
$[31]$	8	3
$[2^2]$	3	2
$[21^2]$	6	2
$[1^4]$	1	1

p	s_p	$\lvert N_G(P)\rvert$	Comment
2	3	8	D_4
3	4	6	S_3

Notes: The Sylow 2-subgroups are generated by the conjugacy class $[2^2]$ and by a certain transposition and a certain 4-cycle:

1. (12) or $(3,4)$; it contains (1324)
2. (13) or (24); it contains (1234)
3. (14) or (23); it contains (1342)

The Sylow 3-subgroup is generated by some element of order 3, say (123). Its normalizer contains the transpositions (12), (23), and (13).

10.2 Alternating Group: A_4

Conjugacy Class	# Elements	Order
$[31]$	8	3
$[2^2]$	3	2
$[1^4]$	1	1

p	s_p	$\lvert N_G(P)\rvert$	Comment
2	1	8	A_4
3	4	6	S_3

Comment: A_4 has no subgroup of order 6.

10.3 Symmetric Group S_5

Conjugacy Class	**# Elements**	**Order**
$[5]$	24	5
$[41]$	30	4
$[31^2]$	20	3
$[32]$	20	6
$[2^21]$	15	2
$[21^3]$	10	2
$[1^5]$	1	1

p	s_p	$\lvert N_G(P)\rvert$	**Comment**
2	15	8	D_4
3	10	6	S_3
5	6	10	D_5

Comments: Sylow 2-subgroup P_2:

$$\{(45), (24)(35), (25)(34), (23)(45), (2435), (2453), (23), ()\};$$

it equals its own normalizer.
Sylow 3-subgroup P_3: $< (235), (253) >$; normalizer has order 6 and equals

$$\{(14)(23), (14)(35), (235), (253), (14)(25), (235), (253), ()\}.$$

Sylow 5-subgroup P_5: $< (12345) >$; normalizer has order 10 and equals

$$\{(13)(45), (14)(23), (25)(34), (15)(24), (12)(35), (12345), \ldots\}.$$

10.4 Alternating Group A_5

Conjugacy Class	**# Elements**	**Order**
$[5]_+$	12	5
$[5]_-$	12	5
$[31^2]$	20	3
$[2^21]$	15	2
$[1^5]$	1	1

p	s_p	$\lvert N_G(P)\rvert$	**Comment**
2	5	12	A_4
3	10	6	S_3
5	6	10	D_5

Comment: Sylow 2-subgroup P_2 is generated by elements from the conjugacy class $[2^21]$: for example, $P_2 = \{(12)(45), (14)(25), (15)(34), ()\}$. Its normalizer has order 12 and is given by

$$\{(143), (345), (153), (145), (12)(45), (14)(25), (15)(34), \ldots\}.$$

The normalizer is generated by a copies of $\mathbf{Z}_2 \times \mathbf{Z}_2$ and $\mathbf{Z}_3$.

11 More Comments on Group Classification

The main feature of the groups that we can successfully analyze have orders whose prime factorizations involve at most three distinct primes with low powers and can be expressed as a semidirect product. It is also within the scope of our techniques to classify the groups of order p^3, where p is a prime. In contrast, there are 2,328 distinct groups of order $2^7 = 128$.

Order	Factor	Total No.	No. Abelian	Semidirect Product	Special Feature
8	2^3	5	3	No	Prime Cubed
12	$2^2 \cdot 3$	5	2	No	A_4
18	$2 \cdot 3^2$	5	2	Yes	Normal Sylow 3
20	$2^2 \cdot 5$	5	2	Yes	Normal Sylow 5
27	3^3	5	2		Prime cubed
28	$2^2 \cdot 7$	4	2	Yes	Normal Sylow 7
30	$2 \cdot 3 \cdot 5$	4	2	Yes	Normal Sylow 3 or 5
42	$2 \cdot 3 \cdot 7$	6	1	Yes	$\mathbf{Z}_2 \to U(7) \times U(3)$
44	$2^2 \cdot 11$	4	2	Yes	Normal Sylow 11
50	$2 \cdot 5^2$	5	2	Yes	Normal Sylow 5
52	$2^2 \cdot 13$	5	2	Yes	Normal Sylow 13
63	$3^2 \cdot 7$	4	2	Yes	Normal Sylow 7
68	$2^2 \cdot 17$	5	2	Yes	Normal Sylow 17
70	$2 \cdot 3 \cdot 7$	4	1	Yes	Normal Sylow 3 or 7
75	$3 \cdot 5^2$	3	2	Yes	Normal Sylow 5
76	$2^2 \cdot 19$	4	2	Yes	Normal Sylow 19
78	$2 \cdot 3 \cdot 13$	6	1	Yes	$\mathbf{Z}_2 \to U(13) \times U(13)$
92	$2^2 \cdot 23$	4	2	Yes	Normal Sylow 23
98	$2 \cdot 7^2$	5	2	Yes	Normal Sylow 7
99	$3^2 \cdot 11$	1	1	Yes	Abelian
117	$3^2 \cdot 13$		Yes		
153	$3^2 \cdot 17$				
171	$3^2 \cdot 19$				
207	$3^2 \cdot 23$				
261	$3^2 \cdot 29$				
279	$3^2 \cdot 31$				
333	$3^2 \cdot 37$				

12 Last Remarks

Yet some more comments about the state of group theory in the late 19th and early 20th centuries from an article by T. Y. Lam of Berkeley that appeared in the Notices of the American Mathematical Society, 1998.

By the 1890s, the known simple groups were the alternating groups A_n, with $n \geq 5$, Jordan's projective special linear groups $\mathrm{PSL}_2(p)$, with $n \geq 5$, and some so-called sporadic simple groups. The American mathematician F.N. Cole found a simple group of order 504, which was recognized

later as $\mathrm{PSL}_2(8)$; that is, over a finite field with $2^3 = 8$ elements. The German mathematician Hölder found all simple groups of order less than 200 in 1892, Cole to order 660 in 1893, and the British mathematician Burnside to order 1092. In this era, Burnside also showed that if the order of a simple groups is even, then it must be divisible by 12, 16, or 56.