8 *p*-Sylows and Simple Groups

12/2: 1. Show that the 2-Sylow subgroups of S_4 and S_5 are isomorphic to D_8, and the 2-Sylow subgroups of A_4 and A_5 are isomorphic to the Klein 4-group.

Proof. Conjugate subgroups are isomorphic, so we need only find one representative 2-Sylow of S_4, S_5, A_4, A_5 and work with each of them. Let's begin.

For S_4, we have $4! = 24 = 2^3 \cdot 3$, and for S_5, we have $5! = 120 = 2^3 \cdot 15$. Thus, in both cases, we're looking for a subgroup of order 8, and the following will suffice.

$$H = \{e, (13), (24), (12)(34), (13)(24), (14)(23), (1234), (4321)\}$$

Noting that $H = \langle (1234), (13) \rangle$ and $D_8 = \langle r, s \rangle$, where $|(1234)| = |r| = 4$ and $|(13)| = |s| = 2$, we can define our isomorphism $\varphi : H \to D_8$ by

$$(1234) \mapsto r \qquad\qquad (13) \mapsto s$$

Everything else follows homomorphically.

Similarly, for A_4, we have $12 = 2^2 \cdot 3$ and for A_5, we have $60 = 2^2 \cdot 15$. Thus, we're looking for a subgroup of order 4 this time, and the following will suffice.

$$H = \{e, (12)(34), (13)(24), (14)(23)\}$$

Here, we define our isomorphism by

$$e \mapsto e \qquad (12)(34) \mapsto (1, 0) \qquad (13)(24) \mapsto (0, 1) \qquad (14)(23) \mapsto (1, 1)$$

□

2. Let H be the subset of $\mathrm{GL}_3(\mathbb{F}_p)$ of matrices of the form

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$$

(a) Prove that H is a p-Sylow subgroup of $\mathrm{GL}_3(\mathbb{F}_p)$.

Proof. We know from Dummit and Foote (2004, p. 35) that

$$\begin{aligned} |\mathrm{GL}_3(\mathbb{F}_p)| &= (p^3 - 1)(p^3 - p)(p^3 - p^2) \\ &= p^9 - p^8 - p^7 + p^5 + p^4 - p^3 \\ &= p^3 \cdot (p^6 - p^5 - p^4 + p^2 + p - 1) \end{aligned}$$

Additionally, each variable x, y, z in the prototypical element of H can take on all p possible values without affecting the status of that matrix as an element of $\mathrm{GL}_3(\mathbb{F}_p)$. This is because that (upper triangular) matrix's determinant will always be the product of its unchanging diagonal entries. Therefore, $|H| = p^3$. It follows by the definition of p-Sylows that H is a p-Sylow of $\mathrm{GL}_3(\mathbb{F}_p)$, as desired. □

(b) Prove that H is not normal.

Proof. To prove that H is not normal, it will suffice to find $h \in H$ and $g \in G$ such that $ghg^{-1} \notin H$. Indeed, if we take

$$h = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \qquad\qquad g = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

then

$$\underbrace{\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}}_{g}\underbrace{\begin{pmatrix}1&0&0\\0&1&2\\0&0&1\end{pmatrix}}_{h}\underbrace{\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}}_{g^{-1}}=\begin{pmatrix}1&0&0\\0&1&0\\0&2&1\end{pmatrix}\notin H$$

as desired. □

(c) Determine the number n_p of p-Sylow subgroups of $\mathrm{GL}_3(\mathbb{F}_p)$.

Proof. Prove 2d and then by Sylow III, take

$$n_p = [G : N_G(H)]$$

From

$$N_G(H) = \left\{ \begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix} | \in \mathrm{GL}_3(\mathbb{F}_p) \right\}$$

That $|N_G(H)| = (p-1)^3p^3$, $|G| = |\mathrm{GL}_3(\mathbb{F}_p)|$. Recall that elements of $\mathrm{GL}_3(\mathbb{F}_p)$ lives in three columns. Treat the columns one by one. The number of choices for the first are p^3-1. The number of choices for the second are p multiples of the first column in $\mathbb{F}_p^3$, p^3-p chosen for the second column. There will be p^3-p^2 choices for the third column. Thus, there are $(p^3-1)(p^3-p)(p^3-p^2)$ ways to choose the columns; this is the order of $|\mathrm{GL}_3(\mathbb{F}_p)|$. Implies that the order

$$\begin{aligned} n_p &= [G : N_G(H)] \\ &= \frac{|G|}{|N_G(H)|} \\ &= \frac{(p-1)^3p^3(p^2+p+1)(p+1)}{(p-1)^3p^3} \\ &= (p^2+p+1)(p+1) \end{aligned}$$

This is a very important computation and Abhijit wants to make sure we really understand it! Write something about it in my OH notes.

If we ever learn Rep theory, we'll learn a different proof of this idea. Denote by U the set of upper triangular matrices. Our proposition 1 is that $N_H(G) = U$. Proposition 2 is $N_U(G) = U$. Why does 2 imply 1? It turns out that $H \triangleleft U$. This is rather subtle. We want to show that $N_G(H) = U$, where H is the **Heisenberg group of matrices**. Check $U \subset N_G(H)$. Approach 1: "Do it" with matrix multiplication and cogue that the diagonal of ghg^{-1} is all ones if $g \in U$. Approach 2: Conjugation in matrix groups is a change of basis. Conjugating by BmB^{-1} is a change of basis from $\{e_1, \dots, e_n\} \mapsto \{Be_1, \dots, Be_n\}$. This does not change how the operator/matrix acts on subspaces. Recall that much of linear algebra can be done in a basis-free sense. □

(d) Determine the normalizer of H.

3. Suppose that P is a normal p-Sylow subgroup of G. Suppose that H is a subgroup of G. Prove that $P \cap H$ is the unique p-Sylow subgroup of H. (Exercise 4.5.33 of Dummit and Foote (2004).)

Proof. To prove that $P \cap H$ is the unique p-Sylow of H, we must show that $P \cap H$ is a p-Sylow of H and that $P \cap H \triangleleft H$. Let's begin.

Since P is a normal p-Sylow, Sylow II implies that P is the only p-Sylow in G. Thus, all p-groups in G are subgroups of P. In particular, since $P \cap H \leq P$, $P \cap H$ is a p-group and, moreover, it must be the maximal p-group (or p-Sylow) in H since any larger p-group would by definition necessarily have elements lying outside of H.

To prove that $P \cap H \triangleleft H$, it will suffice to show that $P \cap H \subset H$ and if $h \in H$ and $x \in P \cap H$, $hxh^{-1} \in P \cap H$. The first claim clearly follows from the set theoretic definition of the intersection. For the second claim, we know that $x \in P$ since $x \in P \cap H$. Thus, since P is normal in G and $h \in H \subset G$, $hxh^{-1} \in P$. Additionally, since $x, h \in H$ and H is a subgroup, we know that the product $hxh^{-1} \in H$. But if $hxh^{-1} \in P, H$, then $hxh^{-1} \in P \cap H$, as desired. □

4. Prove that if $n < p^2$, the p-Sylow subgroup of S_n is abelian. Prove that if $n \geq p^2$, the p-Sylow subgroup of S_n is *not* abelian.

   Proof. Groups of order p^2 and groups of order p are abelian, always?? Counterexample: $p = 3$, S_9 has abelian p-Sylow
   $$\langle (1,2,3,4,5,6,7,8,9) \rangle$$
   □

5. Let N be a normal subgroup of G, and suppose that the largest power of p dividing $|N|$ is equal to the largest power of p dividing $|G|$. Prove that the p-Sylow subgroups of G are precisely the p-Sylow subgroups of N.

   Proof. Every p-Sylow of N is a p-Sylow of G. Suppose for the sake of contradiction that there exists a p-Sylow $Q \subset G$ such that $Q \not\subset N$. Let P be a p-Sylow of N (guaranteed to exist by Sylow I). Sylow II: There exists $g \in G$ such that $gPg^{-1} = Q$. In particular, let $q \in Q$ be such that $q \notin N$. Then $q = gpg^{-1}$ for some $p \in P \subset N$. But this implies that not all $p \in N$ satisfy $gpg^{-1} \in N$, a contradiction. □

6. Prove that there do not exist any simple groups of order p^2q for distinct primes p, q. (*Hint*: Consider the congruence restrictions from Sylow III.)

   Proof. Let G be a group of order $|G| = p^2q$ for p, q distinct primes. Suppose for the sake of contradiction that G is simple. We divide into two cases ($p > q$ and $p < q$).

   First, let $p > q$. Sylow III: $n_p \equiv 1 \bmod p$ and $n_p \mid q$. Thus, $n_p \in \{1, q\}$. If $n_p = 1$, we are done. If $n_p = q$, then $n_p \not\equiv 1 \bmod p$, a contradiction.

   Second, let $p < q$. Sylow III: $n_q \equiv 1 \bmod q$ and $n_q \mid p^2$. Thus, $n_q \in \{1, p, p^2\}$. If $n_q = 1$, we are done. If $n_q = p$, then $n_q \not\equiv 1 \bmod q$. If $n_q = p^2$, then the total number of elements of order q is $n_q(q-1) = p^2(q-1) = p^2q - p^2$. Thus, only p^2 elements of G do not have order q. But since by Sylow I there must exist a p-Sylow of order p^2 in G, these remaining elements will be used up by that p-Sylow. Since there are no more element of G, there is only one p-Sylow in G, which is necessarily normal, a contradiction. □

7. Prove that there do not exist any simple groups of the following orders. (Warning: Not in order of difficulty.)

   (a) (*) 336.

   (b) 1176.

   Proof. $1176 = 2^3 \cdot 3 \cdot 7^2$. We have $n_7 \equiv 1 \bmod 7$ and $n_7 | 24$. Thus, $n_7 = 1, 8$. If $n_7 = 1$, we are done. Now suppose $n_7 = 8$. □

   (c) 2907.

   Proof. $2907 = 3^2 \cdot 17 \cdot 19$. □

   (d) 6545.

   Proof. $6545 = 5 \cdot 7 \cdot 11 \cdot 17$. □