GROUPS OF MEDIUM ORDER

COLTON GRAINGER

9. Assignment due 2018-11-07

9.1. Counting elements [1, No. 6.2.4]. There are no simple groups of order $80, 351, 3875, 5313$.

Demonstration. Suppose for contradiction that G is a simple group of order $80, 351, 3875$, or 5313. Applying Sylow's theorem and counting elements, we see:

- $80 = 2^4 \cdot 5$. Then $n_2 = 5$ and $n_5 = 16$. How many elements in G are *not* of order 5? Precisely $80 - 64 = 16$. Since a Sylow 2 subgroup contains 16 elements (none of which have order 5), we must have $n_2 = 1$, a contradiction.
- $351 = 3^3 \cdot 13$. Then $n_3 = 13$ and $n_{13} = 27$. How many elements are not of order 13? Precisely $351 - 324 = 27$. Yet each Sylow 3-subgroup has 27 elements. So n_3 must be 1, a contradiction.
- $3875 = 5^3 \cdot 31$. Then $n_5 = 31$ and $n_{31} = 125$. Now there are $3875 - 3750$ elements of order 31. We're forced to accept $n_5 = 1$, a contradiction.
- $5313 = 3 \cdot 7 \cdot 11 \cdot 23$. Then $n_7 \geqslant 253$, $n_{11} \geqslant 23$, and $n_{23} \geqslant 231$. Then the number of non-identity elements in G from the Sylow 7, 11, and 23 subgroups must be greater than or equal to 6600—too big! □

9.2. A special case of Burnside's N/C theorem [1, No. 6.2.5]. Let G be a solvable group of order pm, where p is a prime not dividing m, and let $P \in \mathrm{Syl}_p(G)$. If $N_G(P) = P$, then G has a normal subgroup of order m. (How is the hypothesis of the solvability of G used?)

Proof. We observe $n_p = [G : N_G(P)] = m$. So counting elements, there are $m(p-1)$ elements of order $p \in G$. Thus $|G| - m(p-1) = m$ *not* of order p in G. Hall's theorem states that a group G is solvable if and only if for every divisor n of $|G|$ such that $\left(n, \frac{|G|}{n}\right) = 1$, G has a subgroup of order n. Applied to this problem, the m elements in G *not* of order p must constitute a subgroup H.

To show that H is normal, we'll show it's characteristic. Note that every element in $G \setminus H$ has order p, so its image under any $\sigma \in \mathrm{Aut}(G)$ will also have order p. Thus $\sigma(G \setminus H) \subset G \setminus H$. Since σ is a bijection, we see $\sigma(G \setminus H) = G \setminus H$ and, taking complements, $\sigma(H) = H$. So $H \triangleleft G$. □

9.3. Exploiting subgroups of small index [1, No. 6.2.6]. There are no simple groups of order $2205, 4125, 5103, 6545$, or 6435.

Demonstration. Suppose for contradiction that G is a simple group of order $80, 351, 3875$, or 5313. Applying Sylow's theorem and considering subgroups of small index, we see:

- $2205 = 3^2 \cdot 5 \cdot 7^2$. Now $n_7 = 15$, $n_5 \geqslant 21$, and $n_3 \geqslant 7$. We'll only need $n_7 = 15$ for a contradiction. Since $7^2 \nmid n_7 - 1$, there exist distinct Sylow 7-subgroups P and R such that $P \cap R$ is of index 7 in P and R. Now denoting $N = N_G(P \cap R)$, we see $P, R \leqslant N$, thus $7^2 \mid |N|$.
  - Since P and R are distinct, we've got to have $|N| > 7^2$.
  - Now the minimum permissible index of a proper subgroup in G is $\min\{k : |G| \text{ divides } k!\} = 14$.

Date: 2018-11-02.
Compiled: 2018-11-07.

- The above two points imply N has index greater than 14 and less than 45. Thus $|N| = 3 \cdot 7^2$.
- Applying Sylow's theorem to N, $n_7(N) = 1$, which is absurd!—P and R are distinct Sylow 7-subgroups of N.

- $4125 = 3 \cdot 5^3 \cdot 11$. Then $n_5 = 11$. But the minimal permissible index is $\min\{k : |G| \text{ divides } k!\} = 15$. Consider $[G : N_G(P_{11})] = 11$ for a contradiction.
- $5103 = 3^6 \cdot 7$. Then $n_3 = 7$. If $5103 \mid k!$, then $k \geqslant 15$. But $[G : N_G(P_3)] = 7$.
- $6545 = 5 \cdot 7 \cdot 11 \cdot 17$. Then $n_5 = 11$. If $6545 \mid k!$, then $k \geqslant 17$. Yet $[G : N_G(P_5)] = 11$.
- $6435 = 3^2 \cdot 5 \cdot 11 \cdot 13$. Again, $n_5 = 11$. If $6435 \mid k!$, then $k \geqslant 13$. Yet, again, $[G : N_G(P_5)] = 11$. □

9.4. **Permutation representations [1, No. 6.2.7].** There are no simple groups of order 1755 or 5265.

Demonstration. Suppose for contradiction that G is a simple group of order 1755 or 5265. Applying Sylow's theorem and considering normalizers, we see:

- $1755 = 3^3 \cdot 5 \cdot 13$. Then $n_3 = 13$, $n_5 = 351$, and $n_{13} = 27$. Letting G act by conjugation on a Sylow 3-subgroup of index 13, we identify G with its image in S_{13} under the permutation representation afforded by the group action. Since G has no index 2 subgroup, $G \leqslant A_{13}$. Let $H_{13} \in \mathrm{Syl}_{13}(G)$. Because $27 = n_{13} = [G : N_G(H_{13})]$, we have $|N_G(H_{13})| = 65$. Yet also $|N_{A_{13}}(H_{13})| = \frac{1}{2}|N_{A_{13}}(H_{13})| = 78$—a contradiction! For $65 \nmid 78$.
- $5265 = 3^4 \cdot 5 \cdot 13$. Therefore $n_3 = 13$, $n_5 = 351$, and $n_{13} = 27$. As before, let G act by conjugation on a Sylow 3-subgroup of index 13. Again, identify $G \leqslant A_{13}$. Let $H_{13} \in \mathrm{Syl}_{13}(G)$. Then $|N_G(H_{13})| = 195$. But the normalizer of H_{13} in S_{13} has order 78. We ought to have $N_G(H_{13}) \leqslant N_{S_{13}}(H_{13})$, but Lagrange's theorem would imply $195 \mid 78$—a contradiction! □

9.5. **Playing Sylow subgroups [1, No. 6.2.10].** There are no simple groups of order 4095, 4389, 5313, or 6669.

Demonstration. Suppose for contradiction that G is a simple group of order 4095, 4389, 5313, or 6669. Applying Sylow's theorem and considering different p-subgroups, we see:

- $4095 = 3^2 \cdot 5 \cdot 7 \cdot 13$. (This one's anomalous, unless I've made a mistake.) We're forced to have a Sylow 13-normal subgroup.
  - By Sylow's theorem, $n_3 \in \{1, 7, 13, 91\}$, $n_5 \in \{1, 6, 21\}$, $n_7 \in \{1, 15\}$, yet $n_{13} = 1$.
- $4389 = 3 \cdot 7 \cdot 11 \cdot 19$. Let $Q \in \mathrm{Syl}_{11}(G)$. Then $N_G(Q) = 3 \cdot 11$. Let $P \in \mathrm{Syl}_3(N_G(Q))$. Since $3 \nmid 11 - 1$, we have $P \lhd N_G(Q)$. So $Q \leqslant N_G(P)$. By Lagrange's theorem, $11 \mid |N_G(P)|$. Observing that $P \in \mathrm{Syl}_3(G)$, we must have $11 \nmid n_3$ (the number of Sylow 3-subgroups is the index of the normalizer of P). It follows that $n_3 = 7$ or 19.
  - If $n_3 = 7$, then $|N_G(P)| = 3 \cdot 11 \cdot 19$. So $Q \leqslant N_G(P)$. Moreover, $Q \lhd N_G(P)$ (applying Sylow's theorem to $N_G(P)$. But then $|N_G(P)| \neq 3 \cdot 11$—a contradiction.
  - If $n_3 = 19$, then $|N_G(P)| = 3 \cdot 7 \cdot 11$. We see again that $Q \lhd N_G(P)$, leading to the same contradiction (which is what?).
- $5313 = 3 \cdot 7 \cdot 11 \cdot 23$. Let $Q \in \mathrm{Syl}_{11}(G)$. Then $|N_G(Q)| = 3 \cdot 7 \cdot 11$. Let $P \in \mathrm{Syl}_7(N_G(Q))$.
  - For $|G| = 5313$, we must have $n_7(G) = 253$.
  - Applying Sylow's theorem to $N_G(Q)$, we see $P \lhd N_G(Q)$. So $Q \leqslant |N_G(P)|$.
  - Thus 11 divides $N_G(P)$. Moreover, $11 \nmid n_7$—a contradiction! For $11 \mid 253$.
- $6669 = 3^3 \cdot 13 \cdot 19$. We must have $n_{19} = 39$. Now let $Q \in \mathrm{Syl}_{13}(G)$.
  - Then $|N_G(Q)| = 13 \cdot 19$. Let $P \in \mathrm{Syl}_{19}(N_G(Q))$.

- Since $13 \nmid 19-1$, we have a familiar pq group, and $P \lhd N_G(Q)$. Therefore $Q \leqslant N_G(P)$.
- By Lagrange, $13 \mid |N_G(P)|$. But $13 \nmid n_{19}$—a contradiction! For $13 \mid 39$. □

9.6. **Studying normalizers of Sylow subgroups [1, No. 6.2.12].** There are no simple groups of order 9555.

Demonstration. Suppose G is a simple group and $|G| = 9555 = 3 \cdot 5 \cdot 7^2 \cdot 13$.

- We have $n_3 = 91$, $n_5 = 91$ or 1911, $n_7 = 15$, and $n_{13} = 105$.
- Let $Q \in \mathrm{Syl}_{13}(G)$. Let $P \in \mathrm{Syl}_7(N_G(Q))$.
- Then $|N_G(Q)| = 91 = 7 \cdot 13$ as $n_{13} = 105$.
- Sylow's theorem implies $n_7(N_G(Q)) = 1$, so $P \lhd N_G(Q)$.
  - Thence $Q \leqslant N_G(P)$.
- Let $P^* \in \mathrm{Syl}_7(G)$ such that $P \leqslant P^*$.
  - Now $7 = |P| \lneq |P^*| = 7^2$.
  - Thus $N_{P^*}(P) = P^*$.
  - Moreover $N_{P^*}(P) \leqslant N_G(P)$.
- It follows that $\langle Q, P^* \rangle \leqslant N_G(P)$.
- By Lagrange's theorem then $7^2 \cdot 13 \mid |N_G(P)|$.
  - Applying Sylow's theorem to the three cases for the order of $N_G(P)$ (it must be $7^2 \cdot 13$, $7^2 \cdot 5 \cdot 13$, or $3 \cdot 7^2 \cdot 13$) we see $Q \lhd N_G(P)$.
  - So $N_G(P) \leqslant N_G(Q)$.
  - By Lagrange, $7^2 \cdot 13 \mid |N_G(Q)|$.
  - Then $[G : N_G(Q)] \mid 3 \cdot 5$.
  - But Q is a Sylow 13-subgroup, and $n_{13} = 105$, a contradiction. □

9.7. **[1, No. 6.2.22].** Suppose over all pairs of distinct Sylow p-subgroups of G, we have P and R chosen with $|P \cap R|$ maximal. Then $N_G(P \cap R)$ is **NOT** a p-group.

Proof. Since P and R are p-groups, and $P \cap R$ is maximal in both P and R, by Theorem 5.1(5) $P, R \leqslant N_G(P \cap R)$. Now if $N_G(P \cap R)$ was a p-subgroup, then $|P| = |R| = |N_G(P \cap R)|$ (Sylow subgroups are maximal p-groups in G). This would imply $P = R$—a contradiction. So $N_G(P \cap R)$ is *not* a p-subgroup of G. □

9.8. **[1, No. 6.2.25].** Let G be a simple group of order p^2qr where all p, q, r are prime. Then $|G| = 60$.

Proof sketch. By Feit-Thomposon, G must be of even order. Suppose that p is not 2. Then by "Erik's lemma", if G is a group of order $2k$ where k is odd, then G has a normal subgroup. Considering that p^2qr could be written as $2k$ with k odd if $p \neq 2$, we must have $p = 2$.

Without loss of generality, assume $q < r$. We can thus bound $n_r \in \{2q, 4q\}$. We want to show $n_r = 2q$. If we *could do so*, then we'd be able to consider $P \in \mathrm{Syl}_2(G)$. From here, we *could* argue that $p^2 \equiv 1 \pmod{q}$. Thence we'd find $q \mid (p-1)$ or $q \mid (p+1)$. Lastly, we'd observe $q = 2+1$. Moreover, if we could limit n_r to be $2q$, then we'd be forced by congruence, namely $rn + 1 = 2q$, to accept that $r = 5$. □

9.9. **[1, No. 6.3.10].** To exhibit an outer automorphism of S_6. Let

$$\begin{aligned}
t_1' &= (1\,2)(3\,4)(5\,6),\\
t_2' &= (1\,4)(2\,5)(3\,6),\\
t_3' &= (1\,3)(2\,4)(5\,6),\\
t_4' &= (1\,2)(3\,6)(4\,5),\\
t_5' &= (1\,4)(2\,3)(5\,6).
\end{aligned}$$

I claim $t_1', \ldots, t_5'$ satisfies the following relations:

$$\begin{aligned}
(t_i')^2 &= 1 \text{ for all } i, \\
(t_i' t_j')^2 &= 1 \text{ for all } i \text{ and } j \text{ with } |i-j| \geqslant 2, \text{ and} \\
(t_i' t_{i+1}')^3 &= 1 \text{ for all } i \in \{1,2,3,4\}
\end{aligned}$$

Let S' denote the set of the t_i'. We'll verify that elements in S' satisfy the relations for the presentation of S_6 given in lecture:

> What's the Coxeter presentation for $S_n = \langle s_1, \ldots, s_{n-1} \rangle$ where the s_i are simple transpositions $s_i = (i, i+1)$? Consider three cases: $s_i^2 = 1$ (transpositions invert themselves), $s_i s_j = s_j s_i$ if $|i-j| > 1$ (they commute if disjoint), $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$ (they satisfy the braid relation). Whence define the Coxeter matrix $m(s_i, s_i) = 1$, $m(s_i, s_j) = 2$, and $m(s_i, s_{i+1}) = 3$.

Now $(t_i')^2 = 1$ is clear as elements in S' have cycle type $(2,2,2)$. One must perform nontrivial computations to check $(t_i' t_j')^2 = 1$ for all i and j with $|i-j| \geqslant 2$. Yet, one finds that $t_i' t_j'$ has cycle type $(2,2)$ (and thus order 2). Lastly, for $(t_i' t_{i+1}')^3 = 1$ for all $i \in \{1,2,3,4\}$. In this case we see $t_i' t_{i+1}'$ has cycle type $(3,3)$ (thus order 3).

Now elements in S' satisfy the same relations as the simple transpositions in the Coxeter presentation of S_6. Moreover, $\langle S' \rangle = S_6$ as $t_1' t_3' t_5'$ is a 2-cycle and $t_2' t_4' t_5' \rangle$ is a 6-cycle (which is sufficient to generate the simple transpositions).

It follows that $\varphi \to S_6 \to S'$ defined *on generators* by

$$(1\,2) \mapsto t_1', \quad (2\,3) \mapsto t_2', \quad (3\,4) \mapsto t_3', \quad (4\,5) \mapsto t_4', \quad (5\,6) \mapsto t_5'$$

extends to an automorphism of S_6. Observe that φ does not fix conjugacy classes, and thus is and element of $\langle \mathrm{Aut}\,(S_6) \setminus \mathrm{Inn}\,(S_6) \rangle \cong C_2$.

9.10. **[1, No. 6.3.12].** Let S be a set and c a positive integer. Formulate the notion of a free nilpotent group on S of nilpotence class c and prove it has the appropriate universal property with respect to the nilpotent groups of class less than or equal to c.

Formulation. The free nilpotent group on S of nilpotence class c, denoted $N_c(S)$, ought to be given by the presentation $\langle S | \gamma_c(F(S)) \rangle$ where $\gamma_c(F(S)) = [F(S), \gamma_{c-1}(S)]$. From the presentation, there's a surjection $\pi\colon F(S) \to N_c(S)$.

Universal property. Let G be a nilpotent group of class c. Let $\varphi\colon S \to G$ be a map of sets. Then there's a unique $\Psi\colon N_c(S) \to G$ such that the following diagram commutes:

$$\begin{tikzcd}
S \arrow[r, "\pi \circ \iota"] \arrow[dr, "\varphi"'] & N_c(S) \arrow[d, dashed, "\exists! \Psi"] \\
 & G
\end{tikzcd}$$

Proof.[1] Observe $\Phi(\gamma_c(F(S))) \leqslant \gamma_c(G)$ as $\Phi([F(S), \gamma_{c-1}(F(S))]) = [\Phi(F(S)), \Phi(\gamma_{c-1}(F(S)))] \leqslant \gamma_c(G) = 1$. □

[1] I consulted Erik, Hunter, Chris, and `https://terrytao.wordpress.com/2009/12/21/the-free-nilpotent-group/` for this problem. The proof here is hardly sufficient, I'll admit—something to revise.

9.11. **[1, No. 6.3.14].** Prove that $G = \langle x, y : x^3 = y^3 = (xy)^3 = 1 \rangle$ is an infinite group as follows. Let p be a prime congruent to $1 \mod 3$ and let G_p be the non-abelian group of order $3p$. Let $a, b \in G_p$ with $|a| = p$ and $|b| = 3$.

- Both ab and ab^2 have order 3.
- G_p is a homomorphic image of G.
- G is therefore an infinite group, as there are infinitely many primes $p \equiv 1 \mod 3$.

References

[1] D. S. Dummit and R. M. Foote, *Abstract algebra*, 3rd ed. Hardcover; Prentice Hall, 2004 [Online]. Available: http://www.worldcat.org/isbn/0471433349