SYLOW THEORY AND SEMIDIRECT PRODUCTS

COLTON GRAINGER

7. Assignment due 2018-10-24

7.1. **[1, No. 4.5.16].** Let $|G| = pqr$ where p, q and r are primes with $p < q < r$. Then G has a normal Sylow subgroup for either p, q or r.

Given. The number of Sylow subgroups for each prime respectively denoted n_p, n_q, and n_r.

To prove. $n_p = 1$, $n_q = 1$, or $n_r = 1$, forcing a normal Sylow subgroup.

Proof by contradiction. Assume n_p, n_q, and n_r are all strictly greater than 1. To achieve a contradiction, let $k, s, t \in \mathbf{N}$ parameterize

$$n_p = kp + 1, \quad n_q = sq + 1, \quad n_r = tr + 1.$$

For the largest prime r, from $tr + 1 | pq$ we deduce $tr + 1 = pq$. For the middle prime q, we have $sq + 1 = r$ or pr. For the least prime p, we don't have much restriction, and in turn $kp + 1 = q$ or r or qr.

How many non-identity elements are in G? Exactly $pqr - 1$. We'll violate this upper bound. Since the Sylow p, q, r-subgroups are conjugate to each other Sylow subgroup of the same prime, and cyclic, the number of non-identity elements from the Sylow subgroups must be

$$n_r(r - 1) + n_q(q - 1) + n_p(p - 1).$$

But the number of such nonidentity elements is bounded above by $pqr - 1$. Working towards contradiction, we take the most conservative possible values for n_r, n_q, and n_p, and present the inequality

$$pqr - 1 \geq pq(r - 1) + r(q - 1) + q(p - 1).$$

From which it follows that $r + q \geq rq + 1$, which is absurd, as $r, q \geq 3$. □

7.2. **[1, No. 4.5.26].** Let G be a group of order 105. If a Sylow 3-subgroup of G is normal, then G is abelian.

Given. $|G| = 3 \cdot 5 \cdot 7$, with n_p representing the number of Sylow p-subgroups of G.

To prove. If $n_3 = 1$, then G is abelian.

Proof. Arguing by Sylow (N), and assuming $n_3 = 1$, we have

$$n_5 \in \{1, 21\}, \qquad \text{and} \qquad n_7 \in \{1, 15\}.$$

Now, considering the number of nonidentity elements in each cyclic Sylow p group, we can't have any of the following:

- $n_5 = 21, n_7 = 15$ (clearly)
- $n_5 = 21, n_7 = 1$ as then
$$|G| = \underbrace{1}_{\text{order } 1} + \underbrace{2}_{3} + \underbrace{84}_{5} + \underbrace{14}_{7}.$$
- $n_5 = 1, n_7 = 15$ as then
$$|G| = \underbrace{1}_{1} + \underbrace{2}_{3} + \underbrace{4}_{5} + \underbrace{90}_{7}.$$

So $n_3 = n_3 = n_7 = 1$ and $G \cong C_3 \times C_5 \times C_7$, which is abelian. □

Date: 2018-10-18.
Compiled: 2018-10-24.

7.3. **[1, No. 4.5.30].** How many elements of order 7 must there be in a simple group of order 168?

Demonstration. $|G| = 168 = 2^3 \cdot 3 \cdot 7$. Therefore

$$\begin{aligned} n_2 &\in \{3, 7, 21\} \\ n_3 &\in \{4, 7\} \\ n_7 &\in \{8\} \end{aligned}$$

There are $n_7 \cdot (7 - 1) = 42$ elements of order 7. One can show in general the number of elements of order p in $G = pm$ with p not dividing m is given by $n_p(G) \cdot (p - 1)$. □

7.4. **[1, No. 4.5.32].** Let P be a Sylow p-subgroup of H and let H be a subgroup of K. If $P \trianglelefteq H$ and $H \trianglelefteq K$, then P is normal in K. Therefore, if $P \in \mathrm{Syl}_p(G)$ and $H = N_G(P)$, then $N_G(H) = H$.

Given. $P \trianglelefteq H \trianglelefteq K$, with $P \in \mathrm{Syl}_p(G)$

To prove. $P \trianglelefteq K$, also $N_G(N_G(P)) = N_G(P)$.

Proof. Suppose $\sigma \in \mathrm{Aut}(H)$. Say $|P| = p^\alpha$. Then $|\sigma(P)| = p^\alpha$ as well. Normality of $P \in \mathrm{Syl}_p(G)$ implies there's only one Sylow p-subgroup in G. Therefore $\sigma(P) = P$. So P is characteristic in H. With $H \trianglelefteq K$, we have $P \trianglelefteq K$ transitively.

Now specify $H = N_G(P)$. We'll argue $N_G(H) = H$. Since $N_G(P) \cap P = P$, we can set up a trivial application of the diamond isomorphism theorem:

$$\begin{tikzcd}[column sep=small] & N_G(H) \arrow[dl, dash] \arrow[dr, dash, shift left] \arrow[dr, dash, shift right] & \\ P \arrow[dr, dash, shift left] \arrow[dr, dash, shift right] & & N_G(P) \arrow[dl, dash] \\ & P \cap N_G(P) & \end{tikzcd}$$

Having the $\{1 \cdot (P \cap N_G(P))\} = P/(P \cap N_G(P)) \cong N_G(H)/N_G(P)$, we must have $[N_G(N_G(P)) : N_G(P)] = 1$. Given that $N_G(N_G(P)) \subset N_G(P)$, the result follows: normalizers of Sylow P groups are *self-normalizing*.

7.5. **[1, No. 4.5.35].** Let $P \in \mathrm{Syl}_p(G)$ and $H \leq G$. Then $gPg^{-1} \cap H$ is a Sylow p-subgroup of H for some $g \in G$.

Given. $H \leq G$, groups, with $P \in \mathrm{Syl}_p(G)$.

To prove. $\mathrm{Syl}_p(H)$ contains $g^{-1}Pg \cap H$ for a choice of $g \in G$.

Proof. Let H act on the coset space G/P by left multiplication. Now since $|G/P|$ does not divide p, we know $|H(gP)|$ does not divide p.

By orbit-stabilizer [2, p. 9]

$$|\mathrm{Stab}_H(gP)| = |H| \,/\, |H(gP)|\,,$$

so $|\mathrm{Stab}_H(gP)|$ is a subgroup of H containing the maximal power of p in $|H|$.

Say the order of $\mathrm{Stab}_H(gP)$ is $p^a k$. We want to show $k = 1$. So consider

$$\mathrm{Stab}_H(gP) = \{h \in H : hgP = gP\} = \{h \in H : g^{-1}hg \in P\} = \underbrace{H \cap g^{-1}Pg}_{\text{a } p\text{-group}}.$$

So $k = 1$, therefore $\mathrm{Syl}_p(H) \ni \mathrm{Stab}_H(gP) = g^{-1}Pg \cap H$. □

We exhibit that $hPh^{-1} \cap H$ is not necessarily a Sylow p-subgroup of H for any $h \in H$.

Demo. Consider the subgroup $P = \langle (1\,2) \rangle$ where $P \in \mathrm{Syl}_2(S_3)$. For all $h \in \langle (2\,3) \rangle$, we have $H \cap hPh^{-1} = \varnothing$.

7.6. **[1, No. 4.5.44].** Let p be the smallest prime dividing the order of the finite group G. If $P \in \mathrm{Syl}_p(G)$ and P is cyclic, then $N_G(P) = C_G(P)$.

Given. Suppose p is the smallest prime dividing $|G| = p^\alpha m$, where G is finite group and $p \nmid m$. Let $P \in \mathrm{Syl}_p(G)$, and suppose P cyclic.

To prove. $N_G(P) = C_G(P)$.

Proof.[1] Clearly P is abelian, so $P \le C_G(P) \triangleleft NGP$. Consider the quotient [1, Ch. 4.4]

$$N_G(P)/C_G(P) \cong K \le \mathrm{Aut}(P) \cong (\mathbf{Z}/p\mathbf{Z})^\times.$$

Observe $[N_G(P) : C_G(P)]$ divides $p^\alpha(p-1)$. Yet p does not divide $|N_G(P)| / |C_G(P)|$ because

- both N and C contain $P \in \mathrm{Syl}_p(G)$, of maximal prime power order, and
- $C \le N$, leaving no powers of p in the quotient.

We're forced by the "N/C-corollary" to accept that $[N_G(P) : C_G(P)]$ divides $(p-1)$. Now, $[N_G(P) : C_G(P)]$ also divides $|G|$. Because p is the minimal prime divisor of $|G|$, we obtain $[N_G(P) : C_G(P)] = 1$. □

7.7. **[1, No. 4.6.4].** A_n is generated by the set of all 3-cycles for each $n \ge 3$. Cf. [3].

Given. Some $n \ge 3$, an arbitrary permutation $x \in A_n$, and the collection Σ of all 3-cycles in A_n.

To prove. An element $x \in A_n$ can be written as a finite product of terms in Σ.

Proof. First we'll argue: for any $x \in A_n$ that moves at least three elements, there's a $\sigma \in \Sigma$ such that $\sigma^{-1}x$ moves fewer than 3 elements. Intuitively, we might imagine that σ "dampens" the oscillation of x acting on A_n. With the a_i denoting elements of $\{1, \ldots, n\}$, perhaps relabelling, we know x moves a_1 to a_2, and also a_3 somewhere. So let $\sigma = (a_1\, a_2\, a_3)$. Then the product

$$\sigma^{-1}x = (a_1\, a_3\, a_2)(a_1\, a_2\, \ldots = (a_1)\ldots$$

moves strictly fewer elements than x, notably fixing a_1.

To find a representation of an arbitrary $x \in A_n$ we proceed by strong induction on the number of elements that x moves. For the base case, observe that if $x \in A_n$ moves fewer than three elements, then $x = \mathrm{id}$, and we're done. Now take x to move finitely many elements. Now, there's a $\sigma_r \in \Sigma$ such that $\sigma_r^{-1}x$ can be represented as a finite product of 3-cycles in Σ, e.g.,

$$\sigma_r^{-1}x = \sigma_1\sigma_2\cdots\sigma_{r-1}, \quad \text{thus} \quad x = \sigma_1\cdots\sigma_r.$$

Which is what we wanted. □

7.8. **[1, No. 5.1.4].** Let A and B be finite groups and let p be a prime. Any Sylow p-subgroup of $A \times B$ is of the form $P \times Q$, where $P \in \mathrm{Syl}_p(A)$ and $Q \in \mathrm{Syl}_p(B)$. Therefore $n_p(A \times B) = n_p(A)n_p(B)$. We generalize to a direct product of any finite number of finite groups (so that the number of Sylow p-subgroups of a direct product is the product of the numbers of Sylow p-subgroups of the factors).

Given. Let $\{G_i\}_1^n$ be a finite collection of groups, and $G = \prod_1^n G_i$ their direct product. Suppose $|G_i| = p^{a_i}m_i$ with $p \nmid m_i$ for all i.

To prove. We'll generalize immediately and show that the number of Sylow p-subgroups of a direct product is the product of the numbers of Sylow p-subgroups of the factors.

Proof. Note that the coordinate axis subgroups $G_i \triangleleft G$ for all $i \in \{1, \ldots, n\}$. Suppose $P \in \mathrm{Syl}_p(G)$. By the lemma below, it's clear that $\pi_i(P) = P \cap G_i \in \mathrm{Syl}_p(G)_i$. Furthermore, we have as a (subset, and thus as a) subgroup

$$P \le \prod_1^n \pi_i(P).$$

[1] I referred to outside sources (see discussion at https://math.stackexchange.com/questions/1554316, https://math.stackexchange.com/questions/985346, and https://math.stackexchange.com/questions/2229117) to see applications of the "normalizer-centralizer theorem" in the context of this problem.

Then the order of P is given p^α where $\alpha = \sum_1^n a_i$. Yet also

$$\left|\prod_1^n \pi_i(P)\right| = \prod_1^n p^{a_i} = p^\wedge \left[\sum_1^n a_i\right] = p^\alpha.$$

Now P is a subgroup with the same order as the direct product, so

$$P = \prod_1^n \pi_i(P).$$

Now, applying the lemma below, we have a unique representation[2] of $P \in \mathrm{Syl}_p(G)$ as a direct product of Sylow p-subgroups along the coordinate axes, so it follows that $n_p(G) = \prod_1^n n_p(G_i)$. □

Lemma.[3] Suppose $N \triangleleft G$ where G is a group.

(a) For any $P \in \mathrm{Syl}_p(G)$, we have $P \cap N \in \mathrm{Syl}_p(N)$.
(b) For any $K \in \mathrm{Syl}_p(N)$, there's a $P \in \mathrm{Syl}_p(G)$ such that $P \cap N = K$.

7.9. **[1, No. 5.4.15].** If A and B are normal subgroups of G such that G/A and G/B are both abelian, then $G/(A \cap B)$ is abelian.

Given. Groups $A \triangleleft G$ and $B \triangleleft G$ such that G/A and G/B abelian.

To prove. That $A \cap B$ produces an abelian quotient of G.

Proof. By minimality of the commutator G', we have $G' \le A$ and $G' \le B$. Therefore $G' \le A \cap B$. So $G/A \cap B$ is abelian. □

7.10. **[1, No. 5.4.19].** A group H is called perfect if $H' = H$ (i.e., if H is its own commutator subgroup).

(a) Every non-abelian simple group is perfect.

Given. G, a nonabelian, simple group.

To prove. $G = [G, G] =: G'$.

Proof. For contradiction, suppose $G' \lneq G$. The commutator is a proper normal subgroup $G' \triangleleft G$. Because G is simple, the commutator must be trivial. It follows that $G \cong G/G'$ is abelian—absurd! □

(b) If H and K are perfect subgroups of a group G, then $\langle H, K\rangle$ is also perfect. Thence the subgroup of G generated by any collection of perfect subgroups is perfect.

Given. A group G, two perfect subgroups H and K, and a collection of perfect subgroups $\{H_\lambda\}$.

To prove. The join $\langle H, K\rangle$ is perfect, and, in a similar fashion, the join $\langle H_\lambda\rangle$ is perfect.

Proof. Suppose $\langle H, K\rangle$ ain't perfect. Then there exists J such that

$$\langle H, K\rangle' \le J \underset{\neq}{\triangleleft} \langle H, K\rangle$$

where $\langle H, K\rangle/J$ is abelian and nontrivial. We can assume without loss of generality that $H \le J$. But as K is perfect and not quotiented out by J, the group $\langle H, K\rangle/J$ has noncommutative elements generated by representatives[4] from K, a contradiction. So it cannot be that $\langle H, K\rangle \lneq \langle H, K\rangle$. Therefore $\langle H, K\rangle$ is perfect.

Generalizing, $\langle H_\lambda\rangle$ is perfect, for if it's not, we find J such that

$$\langle H_\lambda\rangle' \le J \underset{\neq}{\triangleleft} \langle H_\lambda\rangle$$

with an abelian quotient $\langle H_\lambda\rangle/J$ for contradiction. □

[2] Notice we're *not* claiming to have a unique representation of coordinate axis Sylow subgroups in terms of a subgroup P of the product.

[3] To extend a previous exercise [1, No. 3.4.9].

[4] What vocabulary to use here? Certainly jK is not actually an element in $\langle H, K\rangle/J$, for J is neither normal nor a subgroup of K. But some objects (which?) from K are in the quotient, and they don't commute with each other.

(c) Any conjugate of a perfect subgroup is perfect.

Proof. Conjugation is an automorphism. As a consequence of the definition of *the* commutator subgroup [1, Ch. 5.4], if a group is equal to its commutator subgroup, then any automorphed image of the group will also be equal to its commutator subgroup. □

(d) Any group G has a unique maximal perfect subgroup, and moreover, this subgroup is normal.

Proof (by induction). It's clear that G atleast one perfect subgroup $\{e\}$. If G has any others, we'll find the maximal one as follows.

- Certainly the maximal perfect subgroup is contained in $[G, G]$.
- So also it's also contained in $G^{(2)} = [[G, G], [G, G]]$,
- and generally contained in $G^{(n)} \ldots$
- So the unique maximal perfect subgroup is $\cap_{n=0}^{\infty} G^{(n)}$.

That the unique maximal perfect subgroup, call it $G^{(\infty)}$, is normal, should not be surprising. Extending the argument in (c), each term in the derived series[5] is characteristic in G. Therefore the perfect core[6] $G^{(\infty)}$ is characteristic in G. □

7.11. **[1, No. 5.5.12].** We classify the groups of order 20 (into five isomorphism types).

Demonstration. Consider G a group with $|G| = 20 = 2^2 \cdot 5$. The number of Sylow p-subgroups is found to be $n_2 \in \{1, 5\}$ and $n_5 = 1$. The Sylow 2-subgroups of order 4 will either be isomorphic to V_4 or cyclic. We obtain 3 groups immediately.

$\star$ n_2?	1	5
2-groups?		
cyclic	C_{20}	$C_2 \times C_{10}$
isom. to V_4		D_{20}

We'll list 2 new groups (5 groups in total) and distinguish them each up to isomorphism. Starting with those familiar:

- $C_{20} = \langle x : x^{20} = e \rangle$ exists.
- $C_{10} \times C_2$ also exists as a familiar cartesian product.
  - $C_{10} \times C_2$ has an element $(1, -1)$ of order 2 which prevents an isomorphism to cyclic C_{20}.
- D_{20} has the Coxeter presentation $\langle r, s : r^{10} = s^2 = e, srs^{-1} = r^{-1} \rangle$.
  - $D_{20} \cong C_{10} \rtimes_{\varphi} C_2$ where $\varphi\colon C_2 \to \mathrm{Aut}\,(C_{10})$ is defined (sufficiently, on *generators*) by $\varphi(s)(r) = r^{-1}$.
  - Now $D_{20} \ncong C_{20}$ as D_{20} is not abelian.
  - To distinguish D_{20} from $C_{10} \times C_2$, it's enough to see

$$C_{10} \rtimes_{\varphi} C_2 \ncong C_{10} \rtimes_{\psi} C_2$$

    where $\psi\colon C_2 \to \mathrm{id}_{C_{10}} \subset \mathrm{Aut}\,(C_{10})$ is trivial.
  - Notice $\ker \varphi = \{e\} \neq C_2 = \ker \psi$.

With the theory of semi-direct products, we have the wherewithal to define 2 new groups. They are:

- $C_5 \rtimes_{\gamma} C_4$ where $\gamma\colon C_4 \to \mathrm{Aut}\,(C_5)$ is defined $\gamma(x)(y) = y^{-1}$.
  - This group is not abelian, so is suffices just to check $C_5 \rtimes_{\gamma} C_4 \ncong D_{20}$.
  - Easily done! $\ker \varphi = \{e\} \neq \langle x^2 \rangle = \ker \gamma$.
- $F_{20} := C_5 \rtimes_{\beta} C_4$ with $\beta(x)(y) = y^2$.
  - Now F_{20} is not abelian, so we need only to distinguish F_{20} from the two previous groups.
  - Well $\ker \beta = \{e\} \neq \langle x^2 \rangle = \ker \gamma$.
  - Moreover F_20 has an element (x, id) of order 4 that D_{20} lacks.

[5] https://ncatlab.org/nlab/show/derived+series

[6] `https://groupprops.subwiki.org/wiki/Perfect_core`

We've classified the 5 isomorphism classes of groups of order 20.

7.12. **[1, No. 5.5.18].** If H is any group then there's a group G that contains H as a normal subgroup with the property that for every automorphism σ of H there is an element $g \in G$ such that conjugation by g when restricted to H is the given automorphism σ. That is, every automorphism of H is obtained as an inner automorphism of G restricted to H.

Given. H a group and its group of automorphisms $\mathrm{Aut}(H)$.

To prove. There's a group G with the properties (i) $H \trianglelefteq G$ and (ii) $\forall \sigma \in \mathrm{Aut}(H)$ there's a $g \in G$ such that $ghg^{-1} = \sigma(h)$ for all $h \in H$.

Proof. Consider $G = H \rtimes_{\mathrm{id}} \mathrm{Aut}(H)$ where id is the identity endomorphism on $\mathrm{Aut}(H)$. Now $H \trianglelefteq G$ by definition of the semidirect product. Futhermore, for each $\sigma \in \mathrm{Aut}(H)$, there's $(1, \sigma) \in G$ such that

$$
\begin{aligned}
(1\,\sigma)(h,\,\mathrm{id})(1,\,\sigma)^{-1} &= (1\,\sigma)(h,\,\mathrm{id})(1,\,\sigma^{-1}) \\
&= (\sigma(h)\sigma(1),\,\mathrm{id}) \\
&= (\sigma(h),\,\mathrm{id}).
\end{aligned}
$$

Identifying $\sigma(h)$ with the last term above, the proof is complete. □

7.13. **[1, No. 5.5.23].** Let K and L be groups, let n be a positive integer, let $\rho\colon K \to S_n$ be a homomorphism and let H be the direct product of n copies of L. From [1, No. 5.1.8], we constructed an injective homomorphism ψ from S_n into $\mathrm{Aut}(H)$ by letting the elements of S_n permute the n factors of H. The compositions $\psi \circ \rho$ is a homomorphism from G into $\mathrm{Aut}(H)$. The *wreath product* of L by K is the semidirect product $H \rtimes_{\psi} K$ with respect to this homomorphism and is denoted by $L \wr K$. Note this wreath product depends on the choice of permutation representation ρ of K — if none is given explicitly, then φ is assumed to be the left regular representation of K.

(a) Assume K and L are finite groups and ρ is the left regular representation of K. We find $|L \wr K|$ in terms of $|K|$ and $|L|$.

TODO

(b) Let p be a prime, let $K = L = Z_p$. Suppose ρ is the left regular representation of K. Then $Z_p \wr Z_p$ is a non-abelian subgroup of order p^{p+1} and is isomorphic to a Sylow p-subgroup of S_{p^2}. [The p copies of Z_p whose direct products makes up H may be represented by p disjoint p-cycles; these are cyclically permuted by K.]

TODO

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`

[2] K. Conrad, "Applications of Sylow's Theorem," 2018 [Online]. Available: `http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/sylowapp.pdf`

[3] G. Bergman, "Proof that the group An is simple for all n greater than or equal to 5," Jul. 2000 [Online]. Available: `https://math.berkeley.edu/~gbergman/ug.hndts/A_n_simple.ps`