Some Elementary Proofs:
Burnside's Theorem and Theorems of Baer–Suzuki and Thompson

Notes by Richard Foote

The purpose of Section 1 of this note is to discuss the solvability of certain groups of order $2^a q^b$ (and generalizations) from an elementary, group-theoretic perspective, without the use of character theory. (I employ the term "elementary" to mean proofs that are straightforward consequences of the material in Part I of *Abstract Algebra, third edition*, by Dummit–Foote, [DF].) Section 1 evolved from conversations with David Leep and Hy Ginsberg.

Section 2 was subsequently written to "follow my nose" in seeing how far the ideas in Section 1 could be pushed to obtain an elementary proof of the full Burnside result in the special case of groups of even order. The Appendix, which consists of all the exercises quoted from [DF], was then added in order to make the notes more self-contained.

Section 3, the odd order case of Burnside, was written months after Section 2 in order to complete the picture of Burnside's Theorem from a group-theoretic perspective. I also added it because it includes an elementary proof of a special case of the *Thompson Factorization Theorem*, which closely follows the arguments in the seminal *Normal p-complement Theorem*, [Th]—the latter is where the now ubiquitous *Thompson subgroup* was first introduced. This subgroup is defined and explored in Section 4.4, Exercise 20 of [DF] (reproduced in modified and clarified form in Subsection 3.1). Thus Section 3, although slightly less conceptually "elementary" than the preceding two sections, is nonetheless fully accessible to students conversant with Part I of [DF]. It is intended to serve as a gateway to more advanced techniques in finite group theory emerging from it. Furthermore it provides an opportunity to see both the power and utility of Thompson's ideas and techniques "in action". Indeed, the proof of the special case of Thompson's Theorem is modeled on Thompson's original paper, but with some shortcuts (partly following Aschbacher in [Asc, Section 32]); so readers who master this proof will be well prepared to tackle Thompson's exquisite but challenging opus. As noted at the end of Thompson's paper, [Th] is a self-contained three-page proof of a generalization of the main result of his doctoral dissertation, where he verified the famous 60-year old Frobenius Conjecture!

I lay no claim to the originality of ideas or results in this note, but rather I hope that the organization of these ideas illuminates how one might approach the study of finite group theory in a naturally evolving way. Purely group-theoretic proofs of Burnside's $p^a q^b$ theorem appear both in journals (as cited) and in various text books. I hope that the proofs herein—of Baer–Suzuki and Thompson's Theorems as well as Burnside—are more accessible and self-contained. They are also intended to act as a foretaste of and give insight into the wondrous papers and results in finite group theory pioneered by the greats of the field.

Throughout the notes p and q are primes and all groups considered are finite.

Section 1 — Mason's Theorem.

The main result of this section is to prove the following result, which is motivated by the special case of Burnside's $p^a q^b$ Theorem stated as Exercise 5 in Section 19.2 of [DF]:

5. *Use the ideas in the proof of Philip Hall's Theorem to prove Burnside's $p^a q^b$ Theorem in the special case when all Sylow subgroups are abelian (without use of character theory).*

The main result of this section is:

Theorem A. *Every finite group with an abelian subgroup of index a power of 2 is solvable.*

In particular, this gives Burnside's Theorem in the special case where $p = 2$ and the Sylow q-subgroups for q odd are abelian. The proof is "elementary" inasmuch as it only uses consequences of Sylow's Theorem and facts about p-groups, as in Chapter 6 of [DF].

This result was proven by David Mason around 1975. At that time I was a research student at Cambridge and David was visiting for the semester, having finished his PhD there in 1972. He needed Theorem A to handle a configuration in a paper he was working on, and he asked me why it is true. Together we reduced easily to a minimal counterexample being a non-abelian simple group of even order, and we pondered for a while why this leads to a contradiction. The next day David told me "It's obvious: just use Burnside's Lemma" (Lemma 7, Section 19.2 of [DF]).

In keeping with the notion of "elementary", however, I now give an alternate proof. This proof relies on the Baer–Suzuki Theorem. Aschbacher (in [Asc], 39.6) gives a short, completely elementary proof of the latter result which, for the sake of completeness, I'll distill here at the end of this section, with more detail and notation adapted to our cause. Aschbacher's proof is modeled on a lovely proof by Lyons and Alperin (see [AL]), but Michael circumvents using a chain of subgroups that mimics Alperin's Fusion Theorem. Pre-Lyons proofs of Baer–Suzuki are longer and less translucent (see eg., [Gor], 3.8.2)—see further comments on this proof on the next page, including why it "fits" so well with the spirit of this note.

Recall that $O_p(G)$ is the largest normal p-subgroup of G (see Exercise 37, Section 4.5 of [DF]).

Baer–Suzuki Theorem. *Let p be a prime and let X be a p-subgroup of any finite group G. If $\langle X, X^g \rangle$ is a p-group for every $g \in G$, then $X \leq O_p(G)$.*

As a corollary to the Baer–Suzuki Theorem we get the (familiar) device we need:

Corollary. *If z is an involution in G and $z \notin O_2(G)$, then z inverts some element of G of odd prime order.*

Proof of the Corollary: By the Baer–Suzuki Theorem applied to $X = \langle z \rangle$, there is some conjugate z^g of z such that $\langle z, z^g \rangle$ is not a 2-group. Since the group generated by any two involutions is dihedral (see Exercise 6, Section 1.2 of [DF]), z inverts the (nontrivial, cyclic) rotation subgroup of index 2 in $\langle z, z^g \rangle$. Thus z inverts a rotation of odd prime order, as desired.

Proof of Theorem A: The proof follows the method of proof of Philip Hall's Theorem (see Section 19.2 of [DF]). Let G be a minimal counterexample to the assertion of Theorem A. By hypothesis and the order formulas (Proposition 13, Section 3.2 of [DF]), $G = HP$, where $P \in Syl_2(G)$ and H is abelian; and, replacing H by its $2'$-subgroup if necessary, we may assume H has odd order (i.e., is a Hall complement to P in G). Since the hypotheses pass to normal subgroups and quotient groups, it follows that G is a non-abelian simple group of even order, so both P and H are nontrivial and $O_2(G) = 1$ (see Exercise 10, Section 3.3, as well as Section 3.4 of [DF]).

Let z be an involution in $Z(P)$. By the Baer–Suzuki Corollary, z inverts some element h of odd prime order. Replacing H by a G-conjugate if necessary, we may assume $h \in H$. Let $M = N_G(\langle h \rangle)$. Since H is abelian (the critical hypothesis),

$$\langle H, z \rangle \leq M < G.$$

Since $G = HP$, every $g \in G$ can be written as $g = xy$, where $x \in H$ and $y \in P$; thus $M^g = M^y$. Now

$$\bigcap_{g \in G} M^g \;=\; \bigcap_{y \in P} M^y \;\trianglelefteq\; G.$$

But this intersection is nontrivial since $z \in M$ and $z^y = z$ for all $y \in P$, hence z is in the intersection. This contradicts the simplicity of G, and so completes the proof.

Corollary. Groups of order $2^a q$ and $2^a q^2$ are solvable for every prime q.

Section 1.1 — The Baer–Suzuki Theorem.

We now include a proof of the Baer–Suzuki Theorem. (There does not seem to be an advantage to proving this Theorem just in the "Burnside-type" groups we are considering; and the full Theorem helps to clarify "what is going on" too.) The astute reader will recognize that this elementary proof is essentially a sophisticated adaptation of the methods in the *Studying Normalizers of Intersections of Sylow p-subgroups* subsection of Section 6.2 in [DF], although the proof herein does not even invoke Sylow's Theorem! They will come to better appreciate how simple [sic] ideas burgeon to powerful tools in finite group theory (and this is but one of many "flowers" on this "stem").

Theorem 1.1. *(Baer–Suzuki) Let p be a prime and let X be a p-subgroup of any finite group G. If $\langle X, X^g \rangle$ is a p-group for every $g \in G$, then $X \leq O_p(G)$.*

Let $\mathcal{X}$ be the set of all G-conjugates of X. (In standard notation, $\mathcal{X} = X^G$.) Note that Baer–Suzuki can equivalently be restated as: *If every pair of elements of $\mathcal{X}$ generates a p-group, then $\langle \mathcal{X} \rangle$ is a p-group* (i.e., it is a statement about a conjugacy class of subgroups).

For any collection $\mathcal{Y}$ of subsets of any group G, let $N_G(\mathcal{Y})$ be the subgroup of group elements that permute the sets in $\mathcal{Y}$ among themselves. We (Aschbacher) abuse notation slightly by saying $\mathcal{Y}$ is contained in a subgroup N if each $Y \in \mathcal{Y}$ is contained in N (i.e., formally, $\mathcal{Y}$ is contained in the power set of N). One must be a little careful when talking about normalizers of *subsets*—or collections of subsets—of a group, because, for example, the normalizer of a subset need not contain that subset (and indeed, could just equal the identity, or the center if G is a p-group).

We will need a standard lemma in p-group theory, adapted to certain subsets.

Lemma. Let R be any p-group and let $\mathcal{A}$ be any collection of subsets of R that is stable under conjugation by R. Let $\mathcal{Y}$ be a proper subset of $\mathcal{A}$, and assume $\langle \mathcal{Y} \rangle$ normalizes $\mathcal{Y}$. Then there is some element in $\mathcal{A} - \mathcal{Y}$ that normalizes $\mathcal{Y}$. (Here $\langle \mathcal{Y} \rangle$ is the subgroup generated by all sets $Y \in \mathcal{Y}$.)

Proof of the Lemma: Let $N = N_R(\mathcal{Y})$. If $N = R$, then every element in $\mathcal{A} - \mathcal{Y}$ normalizes $\mathcal{Y}$. (This covers the case $\mathcal{Y} = \emptyset$.) If $N < R$, then since normalizers "grow" in p-groups (Theorem 1, Section 6.1 of [DF]), let g be any element of R normalizing N with $g \notin N$. Since g does not normalize $\mathcal{Y}$, there must be some element $X \in \mathcal{Y}$ such that $X^g \notin \mathcal{Y}$. By hypothesis $\mathcal{Y} \subseteq N$ and g normalizes the latter group, so $X^g \subseteq N$. Since $\mathcal{A}$ is stable under conjugation, $X^g \in \mathcal{A} - \mathcal{Y}$ is the desired element. This completes the proof of the lemma.

Proof of Baer–Suzuki: Recall that $\mathcal{X}$ is the set of all G-conjugates of X. Let $\mathcal{Z}$ be a subset of $\mathcal{X}$ that is maximal with respect to generating a p-group, and let $P = \langle \mathcal{Z} \rangle$. Clearly $\mathcal{Z} \neq \emptyset$ since we may assume $X \in \mathcal{Z}$. If $\mathcal{Z} = \mathcal{X}$ then $P \trianglelefteq G$ so $X \leq O_p(G)$ and the theorem is proven; so by way of contradiction

$$\textit{assume } \mathcal{Z} \textit{ is a proper subset of } \mathcal{X}.$$

By definition of $\mathcal{Z}$ we have

$$\langle \mathcal{Z}, U \rangle \textit{ is not a } p\textit{-group, for all } U \in \mathcal{X} - \mathcal{Z}. \tag{1.1}$$

Over all p-subgroups of G that contain some element of $\mathcal{X} - \mathcal{Z}$ choose Q such that

$$\mathcal{Y} := \{Y \in \mathcal{X} \mid Y \leq P \cap Q\} \quad \textit{has maximum cardinality.}$$

[The reader should keep track that the arguments (and Lemma) are valid even if $\mathcal{Y} = \emptyset$.]
Observe that $\mathcal{Y} \subseteq \mathcal{Z}$, and by (1.1), $\mathcal{Y} \neq \mathcal{Z}$. By construction $P \cap Q$ normalizes $\mathcal{Y}$, hence so does its subgroup $\langle \mathcal{Y} \rangle$.

Let $\mathcal{U}$ be the set of all elements of $\mathcal{X}$ that are contained in Q, so by their definitions we have

$$\mathcal{Y} = \mathcal{Z} \cap \mathcal{U}. \tag{1.2}$$

Since Q, and therefore $\mathcal{U}$, contains an element of $\mathcal{X} - \mathcal{Z}$, it follows from (1.2) that $\mathcal{Y}$ is a proper subset of $\mathcal{U}$. By the Lemma applied to $\mathcal{Y}$ in each of the p-groups P and Q successively (using $\mathcal{Z}$ and $\mathcal{U}$ for $\mathcal{A}$ respectively) we obtain:

$$\textit{there exist} \quad Z \in \mathcal{Z} - \mathcal{Y} \quad \textit{and} \quad U \in \mathcal{U} - \mathcal{Y} \quad \textit{that both normalize } \mathcal{Y}. \tag{1.3}$$

By the overall hypotheses $\langle\, Z, U \,\rangle$ is a p-group, which by (1.3) normalizes $\langle\, \mathcal{Y} \,\rangle$. Thus

$$Q^* := \langle\, \mathcal{Y}, Z, U \,\rangle = \langle\, \mathcal{Y} \,\rangle \langle\, Z, U \,\rangle \textit{ is a } p\textit{-group.}$$

Since $U \in \mathcal{U}$ but $U \notin \mathcal{Y}$, relation (1.2) implies $U \notin \mathcal{Z}$, i.e., Q^* contains the element $U \in \mathcal{X} - \mathcal{Z}$. But $P \cap Q^*$ contains $\mathcal{Y} \cup \{Z\}$, which contradicts the maximality of $\mathcal{Y}$. This completes the proof.

Readers may be interested in [FW], which gives elementary results in a vein similar to Baer–Suzuki.

Section 2 — Burnside's Theorem for Groups of Even Order.

The purpose of this section is to glean from the preceding section "elementary" group-theoretic methods that lead to a proof of the general Burnside Theorem, at least for groups of even order:

Theorem B. Any group of order $2^a q^b$ is solvable, for all odd primes q.

Starting out as in the preceding section, by way of contradiction let G be a counterexample of minimal order. As before, since the hypotheses carry over to all subgroups and quotient groups, G is a simple group of even order all of whose proper subgroups are solvable. Let z be an involution that lies in the center of some Sylow 2-subgroup of G. By the Baer–Suzuki Corollary, z inverts some element h of order q. Let M be a maximal subgroup of G containing $N_G(\langle\, h \,\rangle)$. The rest of the argument involves studying the structure of M and its embedding in G.

Before embarking on the main argument, we first distill fundamental ideas of Baer–Suzuki and Hall that lead naturally to the following independent result, stated in a way that is symmetric in p and q.

An element is called *p-central* in G if it is contained in the center of a Sylow p-subgroup of G.

Proposition. Let K be a group of order $p^a q^b$, where p and q are any distinct primes and $a, b > 0$. Let y be any nontrivial p-central element of K and let x be any nontrivial q-central element of K. If $\langle\, x, y \,\rangle$ has a normal Sylow subgroup for either p or q then K is not simple.

Proof. Choose notation so that $\langle\, x, y \,\rangle$ has a normal Sylow q-subgroup. Let y be in the center of the Sylow p-subgroup P and let x be in the center of the Sylow q-subgroup Q. Let $\mathcal{X} = x^K$ be the K-conjugacy class of x. As in Section 1, by order considerations $K = QP$, so every element of K can be written as $g = cd$, for some $c \in Q$ and $d \in P$. Thus $x^g = x^d$, and hence

$$\mathcal{X} = x^P, \quad \textit{i.e., } P \textit{ acts transitively on } \mathcal{X}.$$

Let $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_r$ be the $\langle\, y \,\rangle$-orbits of $\langle\, y \,\rangle$ acting on $\mathcal{X}$ with $x \in \mathcal{O}_1$, and let $X_i = \langle\, \mathcal{O}_i \,\rangle$, for $1 \le i \le r$; so each X_i is normalized by y. Since the actions of $\langle\, y \,\rangle$ and P on $\mathcal{X}$ commute, P permutes $\{\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_r\}$ and acts transitively on it (this is an easy special case of Exercise 9(a), Section 4.1

of [DF]). Consequently, $|\mathcal{O}_i| = |\mathcal{O}_1|$ and $X_i \cong X_1$, for $1 \le i \le r$. By hypothesis $\langle\, x, y \,\rangle$ has a unique Sylow q-subgroup, which therefore contains $\mathcal{O}_1$, and so X_1 is a q-group. Thus

$$X_i \text{ is a nontrivial } q\text{-group normalized by } y, \text{ for } 1 \le i \le r.$$

Now let $\mathcal{Y}$ be any subset of $\mathcal{X}$ that has maximal cardinality subject to the condition that $\langle\, \mathcal{Y} \,\rangle$ is a q-group normalized by y. Thus $|\mathcal{Y}| \ge |\mathcal{O}_1| \ge 1$. It follows from the maximality of $|\mathcal{Y}|$ that $\langle\, \mathcal{Y} \,\rangle$ normalizes $\mathcal{Y}$. Let R be any Sylow q-subgroup of K containing $\langle\, \mathcal{Y} \,\rangle$, and let $\mathcal{A} = \mathcal{X} \cap R$.

Assume $\mathcal{Y}$ is proper in $\mathcal{A}$. Then by the Lemma in Section 1.1 there is some $x_0 \in \mathcal{A} - \mathcal{Y}$ that normalizes $\mathcal{Y}$. Let $x_0 \in \mathcal{O}_i$ for some i. Since y and x_0 both normalize $\langle\, \mathcal{Y} \,\rangle$, so too does $\langle\, x_0^{\langle y \rangle} \,\rangle = \langle\, \mathcal{O}_i \,\rangle = X_i$. Thus $\langle\, \mathcal{Y} \cup \mathcal{O}_i \,\rangle = \langle\, \mathcal{Y} \,\rangle \cdot X_i$ is a q-group normalized by y, contradicting the maximality of $|\mathcal{Y}|$. This proves $\mathcal{Y} = \mathcal{A} = \mathcal{X} \cap R$.

Let $M = N_K(\langle\, \mathcal{Y} \,\rangle)$, so M contains both the p-central element y and a Sylow q-subgroup R of K. If $M = K$ then $1 \ne \langle\, \mathcal{Y} \,\rangle \trianglelefteq K$ and the proposition holds. Otherwise, as in Section 1, by orders $K = RP = MP$; so Phillip Hall's argument gives that the proper normal subgroup $\cap_{g \in K} M^g = \cap_{d \in P} M^d$ contains y, hence again K is not simple. This completes the proof of the proposition.

Corollary. In the notation of the Proposition, if y normalizes any q-subgroup of K that contains x (or vice versa), then K is not simple.

We will also need some "background" properties of finite solvable groups, that we tag as SOL 1 to SOL 4; these are introduced at the point they are first used. All the proofs of these quoted results are exercises at the same level of difficulty as those in Section 6.1 of [DF], and they require material only from its Part I (some are already exercises in [DF]). We include comments and hints on the proofs of these quoted results at the end of this section.

Returning to the main argument: Throughout this section we let $M_2 = O_2(M)$ and $M_q = O_q(M)$ (see Exercise 37 and its generalization, Exercise 37*, in Section 4.5 of the Appendix). Keep in mind that by their normality, $[M_2, M_q] \le M_2 \cap M_q = 1$, i.e., M_2 and M_q commute. The first needed result is immediate from Exercise 31 in Section 6.1 of [DF]:

$$\text{If } K \text{ is a nontrivial solvable group, then } O_p(K) \ne 1, \text{ for some prime } p. \qquad \text{(SOL 1)}$$

As a consequence of this and the simplicity of G we obtain:

$$\begin{gathered} \text{Either } M_2 \ne 1 \text{ or } M_q \ne 1 \text{ (or both); and} \\ M = N_G(M_p) \text{ whenever } M_p \ne 1, \text{ for } p = 2, q. \end{gathered} \qquad (2.1)$$

Let $T \in Syl_2(G)$ be such that $T \cap M \in Syl_2(M)$, and let $Q \in Syl_q(G)$ with $Q \cap M \in Syl_q(M)$. By the [DF] Exercise 4.5.37 applied in M we have $M_2 \le T$ and $M_q \le Q$. We may further assume $h \in Q$. By construction $N_G(\langle\, h \,\rangle) \le M$, hence

$$Z(Q) \le M. \qquad (2.2)$$

Next, as in Section 1, we argue that

$$M \text{ does not contain either a Sylow 2-subgroup or Sylow } q\text{-subgroup of } G. \qquad (2.3)$$

Otherwise suppose M contains either T or Q. Then by order considerations $G = MQ$ or $G = MT_1$ respectively, where $z \in Z(T_1)$ for some $T_1 \in Syl_2(G)$. Then use the Phillip Hall intersection argument to show G is not simple, a contradiction. (The reader should check the details.)

In order to unravel the structure of certain subgroups of M, we state our second property of solvable groups, which is Exercise 34 in Section 6.1 of [DF]:

$$\begin{gathered}\textit{If } K \textit{ is a solvable group with no nontrivial normal subgroup of order prime to } p,\\ \textit{then } C_K(O_p(K)) = Z(O_p(K)), \quad \textit{and so} \quad C_K(O_p(K)) \le O_p(K).\end{gathered} \tag{SOL 2}$$

[Remark: In light of (a new) Exercise 37* in Section 4.5 of the Appendix, the "*...with no nontrivial...*" hypothesis on the solvable group K can be stated more succinctly as: "*... with* $O_{p'}(K) = 1$,". Assuming the hypothesis of SOL 2, we conclude that K acts by conjugation as automorphisms of $O_p(K)$ with $Z(O_p(K))$ as the kernel of this action (cf. Section 4.4 of [DF]); so, in many respects, $O_p(K)$ "controls" much of the structure of K itself. In particular, $|K| \le |\mathrm{Aut}(O_p(K))| \cdot |Z(O_p(K))|$. This is one facet of the importance of $O_p(K)$ in the general structure theory of finite groups.
SOL 2 is a special case of the *Fitting Subgroup Theorem*, which is Exercise 34* at the end of the Appendix. The latter exercise is used in Section 3.]

Continuing the main argument, first suppose $M_2 = O_2(M) = 1$. By (2.1), $M_q \ne 1$, and since $M_q \le Q$, we have $Z(Q)$ centralizes M_q. Thus (2.2) and SOL 2 imply $Z(Q) \le C_M(M_q) \le M_q$. In this case the 2-central involution $y = z$ normalizes the q-group M_q containing $Z(Q)$, and the Corollary gives a contradiction. Since $M_2 \le T$ this proves (via (2.1)):

$$M_2 = O_2(M) \ne 1, \quad \textit{and so} \quad Z(T) \le N_G(M_2) = M. \tag{2.4}$$

Next suppose $M_q = O_q(M) = 1$. Since $M_2 \le T$, we have $Z(T)$ centralizes M_2. Thus (2.4) and SOL 2 imply $Z(T) \le C_M(M_2) \le M_2$. Now by (2.2), $Z(Q)$ normalizes the 2-group M_2 which contains $Z(T)$, and the Corollary again gives a contradiction. Thus we must also have

$$M_q = O_q(M) \ne 1. \tag{2.5}$$

At this point we could in invoke (or paraphrase) "structural" results of Helmut Bender (in [Be] or [Ma]) that show that the minimal counterexample group G cannot possess the maximal subgroup M with both M_2 and M_q nontrivial. Rather than do this, however, we pursue our "follow your nose" method further and see what can be said about $\langle\, t, x \,\rangle$ generated by certain 2- and q-central elements of M. This will ultimately enable us to significantly distill the portions of Bender's argument that we need.

Henceforth (relying on (2.2) and (2.4)) let

$$H = \langle\, t, x \,\rangle, \quad \textit{where } t \textit{ is an involution in } Z(T) \textit{ and } x \textit{ is an element of order } q \textit{ in } Z(Q).$$

(We now use this t instead of z as our 2-central element; the original z and h play no further role.) By the Proposition, H does not have either a normal Sylow 2- or q-subgroup; in particular,

$$t \notin M_2 \qquad \textit{and} \qquad x \notin M_q. \tag{2.6}$$

In order to unravel the structure of H we adopt a "Chinese Remainder Theorem" approach and determine the image of H in M/M_2 (for the q-structure) and then in M/M_q (for its 2-structure).

Let $\widetilde{M} = M/M_2 = M/O_2(M)$. By Exercise 37(d) in Section 4.5 of [DF], we have $O_2(\widetilde{M}) = \widetilde{1}$. Thus by SOL 2,

$$\widetilde{Z(Q)} \le Z(\widetilde{Q}) \le O_q(\widetilde{M}).$$

(Keep in mind that although $\widetilde{O_q(M)} \le O_q(\widetilde{M})$, in general the latter subgroup is larger.) Thus $\widetilde{x}$ lies in the abelian group $Z(O_q(\widetilde{M}))$ which is normalized by the involution $\widetilde{t}$. Thus $\widetilde{x}$ and $(\widetilde{x})^{\widetilde{t}}$

commute and generate a group isomorphic to either Z_q (when $\widetilde{t}$ normalizes $\langle\,\widetilde{x}\,\rangle$) or $Z_q \times Z_q$ (when $\widetilde{t}$ does not normalize $\langle\,\widetilde{x}\,\rangle$ — it interchanges the two Z_q factors). We eliminate the first of these two possibilities.

If the involution $\widetilde{t}$ normalizes $\langle\,\widetilde{x}\,\rangle$, then $\widetilde{t}$ either centralizes or inverts the subgroup $\langle\,\widetilde{x}\,\rangle$ (these are the only automorphims of order 1 or 2 of Z_q). Assume the former scenario occurs. Then $\langle\,\widetilde{x}\,\rangle$ likewise centralizes $\langle\,\widetilde{t}\,\rangle$. By taking preimages in M, it follows that x normalizes the 2-group $M_2\langle\,t\,\rangle$, and the Corollary gives a contradiction.

Similarly, if $\widetilde{t}$ inverts $\langle\,\widetilde{x}\,\rangle$, then again by taking preimages in M, we see that t inverts some subgroup of prime order q in the group $M_2\langle\,x\,\rangle$. Since $\langle\,x\,\rangle$ is a Sylow q-subgroup of the latter group, t inverts (hence normalizes) some conjugate of $\langle\,x\,\rangle$. Again, the Corollary gives a contradiction. These arguments prove:

$$H/(H \cap M_2) \;\cong\; \widetilde{H} \;=\; \big(\langle\,\widetilde{x}\,\rangle \times \langle\,\widetilde{x}\,\rangle^{\widetilde{t}}\big)\langle\,\widetilde{t}\,\rangle \;\cong\; Z_q \wr Z_2. \tag{2.7}$$

Since factoring M by the 2-group M_2 preserves the Sylow q-structure, the Sylow q-subgroups of H are of type $Z_q \times Z_q$. Also, the complete preimage in H of the Sylow q-subgroup of $\widetilde{H}$ is a subgroup of index 2 in H. Since H has a subgroup, H_0, of index 2, a Sylow 2-subgroup of H cannot have order 2 or 4 — otherwise it follows easily that H_0, hence also H, would have a normal Sylow q-subgroup, contrary to the Proposition. (Note that by the Corollary, t does not normalize any Sylow q-subgroup of H; rather some element in the *coset* tM_2 normalizes a Sylow q-subgroup of H.)

Next let $\widehat{M} = M/M_q$. As before, by SOL 2 we have $\widehat{t} \in Z(O_2(\widehat{M}))$, and then likewise $\langle\,(\widehat{t})^{\langle\,\widehat{x}\,\rangle}\,\rangle$ is an elementary abelian 2-group. Also, since t inverts some element y of order q in H, we have $[\widehat{t},\widehat{y}] \in O_2(\widehat{M}) \cap \langle\,\widehat{y}\,\rangle = \widehat{1}$. Since $\widehat{t}$ both inverts and centralizes $\widehat{y}$ in the quotient group $\widehat{H}$, we must have $\widehat{y} = \widehat{1}$. This means that the $Z_q \times Z_q$ Sylow q-subgroup of H maps to just the cyclic subgroup $\langle\,\widehat{x}\,\rangle$ in $\widehat{H}$. Putting this together with (2.7) gives

$$\begin{gathered} H/(H \cap M_q) \;\cong\; \widehat{H} \;=\; \langle\,(\widehat{t})^{\langle\,\widehat{x}\,\rangle}\,\rangle\langle\,\widehat{x}\,\rangle \;\cong\; E_{2^m} Z_q, \\ \textit{and so} \quad H \cap M_2 \cong E_{2^{m-1}}, \quad \textit{for some } m \geq 3. \end{gathered} \tag{2.8}$$

Results (2.7) and (2.8) are sufficient to give the Sylow structure and indeed the isomorphism type of our H (depending on m). I had hoped that we could then use this, together with Baer–Suzuki–Hall arguments, to obtain an easy contradiction. That goal has not been realized (remains open). Fortunately we now have enough information to extract and simplify sub-arguments from [Be] and [Ma] to get a contradiction in fairly short order. But this involves quoting two additional facts, whose proofs are also outlined (as exercises with hints) at the end of this section.

The next of these quoted result is the following (where Exercise 37* in Section 4.5 of the Appendix lists the relevant notation and elementary properties of the subgroups involved):

If K is a solvable group, then $O_{p'}(N_K(P)) \leq O_{p'}(K)$, for every p-subgroup P of K. (SOL 3)

In the special case when $|K| = p^a q^b$ for any distinct primes p, q, SOL 3 says equivalently that if D is any q-subgroup of K with $D \trianglelefteq N_K(P)$, then $D \leq O_q(K)$.

SOL 3 is one of the foundational results in the study of *p-local subgroups* of finite groups, where a *p-local subgroup of any finite group A* is defined to be the normalizer of any nontrivial p-subgroup of A. SOL 3 says that in a (finite) solvable group K, the normal p'-subgroups of p-local subgroups of K get "pushed-down" into the largest normal p'-subgroup of the whole group K. This critical "local-global" embedding property has far-reaching ramifications in the study of general finite groups. The next result, (2.9)—and its proof—is a particular exemplar of the latter assertion.

Before stating SOL 4, we first use SOL 3 to obtain a crucial embedding property:

$$M \text{ is the unique maximal subgroup of } G \text{ that contains } M_2M_q. \tag{2.9}$$

To prove this let N be any maximal subgroup of G containing M_2M_q and let N_2 and N_q denote $O_2(N)$ and $O_q(N)$ respectively. The steps of the proof exhibit delightful symmetry between M and N as well as between 2 and q.

First apply SOL 3 to the 2-group $P = M_2$ in the solvable group $K = N$, using the fact that $M_q \trianglelefteq N_N(M_2)$, to get $M_q \leq N_q$. Then symmetrically apply SOL 3 to the q-group $P = M_q$ in the solvable group $K = N$, using the fact that $M_2 \trianglelefteq N_N(M_q)$, to get $M_2 \leq N_2$. Now since N_2 and N_q commute, from the two previous containments we get $N_q \leq N_G(M_2) = M$ and $N_2 \leq N_G(M_q) = M$, that is, N_2N_q is contained in M. By the completely symmetric argument with the roles of M and N and their corresponding subgroups interchanged, we see that $N_q \leq M_q$ and $N_2 \leq M_2$ (using that (2.1) holds symmetrically for N in place of M). Thus $N_q = M_q$ and so we get $N = N_G(N_q) = N_G(M_q) = M$, which establishes (2.9).

Next, by (2.8) we have that $H \cap M_2$ contains a Klein fourgroup W. Moreover, by its proof, $\widehat{W} \leq Z(O_2(\widehat{M})) \cap \widehat{M}_2 \leq Z(\widehat{M}_2)$. Since the homomorphism $\widehat{\ } : M \to M/M_q$ restricts to an isomorphism between the Sylow 2-subgroups of M and $\widehat{M}$, we have $W \leq Z(M_2)$. Thus for every $w \in W$ we have $M_2 \leq C_M(w)$ (and $M_q \leq C_M(w)$ since $w \in M_2$). By (2.9) we obtain

$$C_G(w) \leq M, \quad \text{for every } w \in W - \{1\}. \tag{2.10}$$

We require a final general result, which is stated only in the highly restricted (and easy to prove) form that we need: Let q be any odd prime. In any group K:

$$\begin{gathered}\text{If } F \text{ is a } q\text{-group that is normalized by any Klein fourgroup } W, \text{ then} \\ F = \langle\, C_F(w) \mid w \in W - \{1\} \,\rangle.\end{gathered} \tag{SOL 4}$$

Since W has exactly three nonidentity elements (involutions), F is generated by their three centralizers (although this extra fact is not utilized). This "background" result is labeled SOL 4 because it is only a statement about the solvable group FW. More comments on SOL 4 appear in the "Remarks" subsection following the proof.

The final step: By (2.3) the Sylow 2-subgroup $T_0 = T \cap M$ of M is proper in the Sylow 2-subgroup T of G. Since normalizers "grow" in p-groups, there is some $s \in T - T_0$ with s normalizing T_0. (Note that $s \notin M$ so $M^s \neq M$.) Since $T_0 = T_0^s$ we have that W, W^s, M_2 and M_2^s are all contained in $M \cap M^s$, where W is, as above, a Klein fourgroup contained in $H \cap Z(M_2)$. Apply SOL 4 to $F = M_q^s$, which is a q-group normalized by W in the group $K = M^s$. This gives

$$M_q^s = \langle\, C_{M_q^s}(w) \mid w \in W - \{1\} \,\rangle.$$

By (2.10) we then have $M_q^s \leq M$. Thus $M_2^sM_q^s \leq M$ (equivalently, $M_2M_q \leq M^{s^{-1}}$), and so by (2.9), $M = M^s$, a contradiction. This completes the proof of Theorem B.

Remarks on the proofs of SOL 1 – SOL 4.

SOL 1: As observed, SOL 1 is immediate from Exercise 31 in Section 6.1 of [DF] (see Appendix).

SOL 2: This is Exercise 34 in Section 6.1 of [DF]. The [Hint] appearing in the book should be revised—I include such a revision in the Appendix. SOL 2 is a special case of the *Fitting Subgroup Theorem*, which is Exercise 34* immediately after Exercise 34 in the Appendix. The combination

of SOL 2 and SOL 3 is the beginning of many deep and powerful tools in the general structure theory of finite groups.

SOL 3: Proofs of this statement generally rely on the so-called *Thompson $A \times B$–Lemma*, but the following [with hint] is a more self-contained argument.
Prove SOL 3 by (double) induction, first on $|K|$, and, subject to this, on $|P^* : P|$, where P^* is a Sylow p-subgroup of K containing P.
[Hint: By induction as above, let K be a counterexample of minimal order and, subject to this, with P a p-subgroup of K of *maximal* order for which the conclusion fails. First use Exercise 20 in Section 6.1 of [DF] (in the Appendix) to show that by minimality $O_{p'}(K) = 1$. Let $N = N_K(P)$ and $Q = O_{p'}(N)$ (so $Q \neq 1$ by hypothesis). Show that $Q = O_{p'}(C_K(P))$. Use SOL 2 to show that P does not contain $O_p(K)$; in particular, $P \neq P^*$ (which is the "base case" of the induction on index). Let $P_1 = N_{PO_p(K)}(P) \leq N$. Argue that $P < P_1$ and $Q \trianglelefteq C_K(P_1)$ to show that P_1 is a counterexample in K of *larger* p-power order, a contradiction.]

SOL 4: This is a special case of a more general "generation" result about abelian p-groups W of rank $n > 1$ acting on groups F of order relatively prime to p — the latter groups are then generated by centralizers of subgroups of W of rank $n-1$ (this generalization is discussed in Section 3). The SOL 4 special case — the only one we need in Section 2 — is however much easier to prove.
[Hint: One completely elementary way of proving SOL 4 is as follows: Let

$$F_0 = \langle\, C_F(w) \mid w \in W - \{1\} \,\rangle, \qquad F_1 = N_F(F_0), \qquad \overline{F_1} = F_1/F_0.$$

Note that W acts on both F_0 and F_1, hence also on $\overline{F_1}$. Since normalizers "grow" in q-groups, check that $F_0 = F$ if and only if $\overline{F_1} = \overline{1}$. Then use Exercise 20(b) in Section 6.1 to show that each $w \in W - \{1\}$ acts by conjugation as a *fixed point free automorphism on* $\overline{F_1}$ (see Exercise 23 of Section 1.6 — in the Appendix — for the definition and relevant properties of such automorphisms). Deduce that since (by the exercise) all three involutions w_1, w_2 and $w_1 w_2$ in W invert every element of $\overline{F_1}$ we must have $\overline{F_1} = \overline{1}$, as needed.

A more "classical" approach to proving SOL 4 is as follows: First reduce to the case where one may assume F is an elementary abelian q-group by: factor out the Frattini subgroup, $\Phi(F)$, of F and use Exercises 20 and 26 in Section 6.1 of [DF] to show that if the result holds for $F/\Phi(F)$ in place of F then it holds for F too. (Note that the characteristic subgroup $\Phi(F)$ is normalized by W, so W acts on the q-group $F/\Phi(F)$.) This reduces the proof of SOL 4 to the case when F is an elementary abelian q-group i.e., F is a finite dimensional vector space over the field $\mathbb{Z}/q\mathbb{Z}$. SOL 4 then follows immediately by simultaneously diagonalizing the matrices representing the elements of W (why?).

Alternatively, one can avoid using linear algebra in the case where F is elementary abelian by explicitly decomposing F into W-invariant subgroups (which are eigenspaces) as follows: Write F in additive notation. Fix any $w \in W - \{1\}$ and define:

$$F^+ = C_F(w) = \{v + v^w \mid v \in F\} \quad \textit{and}$$
$$F^- = \{v \in F \mid v^w = -v\} = [F, w] = \{v - v^w \mid v \in F\},$$

and check that these are W-invariant subgroups. Show $F = \langle\, F^+, F^- \,\rangle \cong F^+ \times F^-$ (this is where we need q to be odd). Finally, write $W = \langle\, w, u \,\rangle$ for some involution u. Likewise consider the action of u on F^-, i.e., decompose F^- into its $+/-$ subgroups under the action of u on it; and then deduce that F^- is generated by the subgroups $C_{F^-}(u)$ (which is its plus space for u) and $C_{F^-}(wu)$ (i.e., the minus space for u acting on F^- is the plus space for wu), as needed.]

Additional thoughts

1. Formulate an independent version (Proposition) of display (2.9) for more general groups G and maximal subgroups M of G. What hypotheses on G, M do you need? Does essentially the same argument then work for your G?

2. Try re-working the methods in this section to prove that a finite group with a nilpotent subgroup of index a power of 2 is solvable. (Again, this could be deduced immediately from Burnside's Lemma, using character theory.)

3. A closer examination of the proof of Theorem B shows that only the existence of a fourgroup W in $Z(M_2)$ is needed to complete the proof, starting from SOL 3 onward. Can you shorten the discussion of the structure of H (i.e., the proof of (2.8)) to extract this existence result only?

4. As a more difficult project: Do these ideas extend to give a group-theoretic proof of Burnside's Lemma itself, for any finite group that has a conjugacy class of size a power of 2? (I do not know if the latter has been done before.)

Section 3 — Burnside's Theorem for Groups of Odd Order.

This section rounds out the notes by giving a proof of the following case of Burnside's Theorem, stated in a slightly more general form than just the odd order version.

Theorem C. Assume p, q are primes with $\{p, q\} \neq \{2, 3\}$. Then any group of order $p^a q^b$ is solvable.

The order hypothesis, for $p < q$, is clearly equivalent to p and q being both odd or $p^a q^b = 2^a q^b$ for some prime $q \geq 5$ (i.e., $pq \neq 6$). The obstruction to the argument in Section 2 working for odd order groups is that for odd primes p and nontrivial p-central elements x, when attempting at the outset to apply the Baer–Suzuki Theorem in a minimal counterexample G, the structure of $\langle\, x, x^g \,\rangle = D$ is not readily determined (in the case when $p = 2$ it is a dihedral subgroup). Indeed, it is possible that $D = G$, so we cannot assert that $O_q(D) \neq 1$, which was the pivotal starting point for both Sections 1 and 2.

Although virtually all of the steps in Section 2 are utilized in this proof as well, the one additional tool needed is a special case of the so-called *Thompson Factorization Theorem*. This Theorem is discussed and proved (in the restricted, easier version we need) in Subsection 3.1. Fortunately the main proof, as well as that of Thompson's Theorem, invoke only one additional "external" result, SOL 4*, which is a generalization of SOL 4 that was already alluded to in the discussion of SOL 4 at the end of Section 2. A proof of the SOL 4* is outlined at the end of this section—and like the other quoted "SOL–facts", it reduces to accessible exercises. So again, Section 3 is essentially self-contained as intended (although the reader is also charged with doing some easy elementary [DF]-level exercises that clarify certain steps of the proof, but are of independent interest).

The proof of Theorem C now begins as in Section 2: Throughout this proof G is a counterexample of minimal order, hence is a non-abelian simple group all of whose proper subgroups are solvable. Note that the Proposition at the beginning of Section 2 remains valid for $G = K$ as well.

Let M be any maximal subgroup of G. Adopt the same notation as in Section 2: $O_p(M) = M_p$ and $O_q(M) = M_q$. Early in the proof of Theorem B we showed that for a certain M produced via the Baer–Suzuki Corollary, both M_p and M_q are nontrivial (displays (2.4) and (2.5)). The ensuing arguments then lead to a contradiction. This line of reasoning can also be modified in this situation to yield the following:

$$\textit{For every maximal subgroup } M\textit{, exactly one of } M_p \textit{ or } M_q \textit{ is nontrivial.} \tag{3.1}$$

By way of contradiction assume $M_p \neq 1$ and $M_q \neq 1$. We sketch how a contradiction is achieved by following the arguments from (2.5) onward, showing only what modifications need to be made—the details are left for the reader (who may simply wish to rewrite the portions of Section 2 to cover any minimal counterexample G to Burnside—regardless of even/odd parity—satisfying (2.4) and (2.5)).

To prove (3.1) first choose notation so that $p < q$ (so p plays the role of 2). Let $P \in Syl_p(G)$ be such that $P \cap M \in Syl_p(M)$ and let $Q \in Syl_q(G)$ be such that $Q \cap M \in Syl_q(M)$. Then $M_p \leq P \cap M$ and $M_q \leq Q \cap M$, so

$$Z(P) \leq N_G(M_p) = M \qquad \textit{and} \qquad Z(Q) \leq N_G(M_q) = M. \tag{3.1a}$$

Verify, by the same argument in Section 2, that (2.3) holds for M now too:

$$M \textit{ does not contain either a Sylow } p\textit{-subgroup or Sylow } q\textit{-subgroup of } G. \tag{3.1b}$$

Again let

$$H = \langle\, t, x \,\rangle, \quad \textit{where } t \textit{ is an element of order } p \textit{ in } Z(P) \textit{ and } x \textit{ is an element of order } q \textit{ in } Z(Q).$$

Verify that the same arguments, mutatis mutandis, yield that the Sylow subgroups of H are both elementary abelian, i.e., isomorphic to E_{p^m} and E_{q^n} respectively.

Show next that

$$H \cap M_p \cong E_{p^{m-1}}, \quad \textit{for some } m \geq 3, \tag{3.1c}$$

where the assertion that $m \geq 3$ requires Exercise 2 at the end of this section to eliminate the possibility that $m = 2$.

Next verify that the Bender argument giving (2.9) also holds verbatim once 2 is replaced by p:

$$M \textit{ is the unique maximal subgroup of } G \textit{ that contains } M_pM_q. \tag{3.1d}$$

Finally, arrive at the contradiction by the reasoning following (2.9): This is where we need a generalization of SOL 4 (which is stated in a form that is even more general than when A is just E_{p^2}, since it will be needed in this generality in the proof of Thompson's Theorem). For p and q any distinct primes:

$$\begin{gathered}\textit{if } F \textit{ is a } q\textit{-group normalized by any nontrivial elementary abelian } p\textit{-group } A,\\ \textit{then} \quad F = \langle\, C_F(B) \mid B \leq A \text{ with } |A : B| = p \,\rangle.\end{gathered} \tag{SOL 4*}$$

SOL 4 is the special case where $A \cong E_4$. As in Section 2, remarks at the end of this section sketch how to reduce SOL 4* to "elementary" exercises. Finally, the adapted argument in Section 2 immediately after SOL 4 leads to a contradiction. This proves (3.1).

Returning to the main argument, for the next results we remove the notational restriction that $p < q$. Now easily eliminate the "Baer–Suzuki configuration" as we did at the outset of Section 2:

$$\textit{No nontrivial } p\textit{-central element normalizes a nontrivial } q\textit{-subgroup of } G. \tag{3.2}$$

By way of contradiction assume the nontrivial p-central element z normalizes the nontrivial q-subgroup R. Let M be a maximal subgroup containing $N_G(R)$. Let Q be a Sylow q-subgroup of G such that $R \leq Q \cap M \in Syl_q(M)$. Then $Z(Q) \leq N_G(R) \leq M$. By (3.1) either $M_p = 1$ or $M_q = 1$. If $M_p = 1$, then SOL 2 implies $Z(Q) \leq C_M(M_q) \leq M_q$, which leads to a contradiction by the Corollary in Section 2 applied to $y = z$ normalizing M_q. If on the other hand $M_q = 1$, then $M_p \neq 1$. Let P be a Sylow p-subgroup of G such that $P \cap M \in Syl_p(M)$. Likewise $Z(P) \leq N_G(M_p) = M$

and so SOL 2 forces $Z(P) \leq C_M(M_p) \leq M_p$. Again a contradiction is achieved by applying the same Corollary to a nontrivial element of $Z(Q)$ normalizing M_p (with p and q interchanged in the application).

[*Comment:* Coming up is the point where we use the Thompson subgroup $J(P_1)$, for P_1 any nontrivial p-subgroup of G. We need Theorem 3.1, stated and proved in Subsection 3.1. The arguments in this proof of Theorem C do not require the specific definition of the "J-subgroup", but only that $J(P_1)$ is *some* nontrivial characteristic subgroup of P_1 that satisfies the conclusion of Theorem 3.1 for every P_1 that is Sylow in a suitable proper subgroup K of G. So we defer actually defining the Thompson subgroup until Subsection 3.1. (In the proof of Theorem C one can think of $J(P_1)$ as just being "like" $Z(P_1)$ or P_1' etc. for these purposes.)

The ensuing arguments are strongly based on those in Section 6.2 of [DF], especially its *Studying Normalizers of Intersections of Sylow p-subgroups* subsection. In the parlance of modern finite group theory they fall under the rubric of *"pushing-up"*, where we encounter chains: J char $P_1 \trianglelefteq P_2$ and use "transitivity of normality for characteristic subgroups" to "push up" the normalizer of J to contain the larger group P_2 (see Section 4.4 of [DF]).]

Let $P \in Syl_p(G)$, let t be any element of order p in $Z(P)$, and let M be any maximal subgroup containing P. It is immediate from (3.2) that

$$M_q = 1 \quad \text{and} \quad C_G(t) = P. \tag{3.3}$$

Thus M satisfies the hypotheses of Theorem 3.1, and so

$$M = N_G(J(P)). \tag{3.4}$$

We started with M any maximal subgroup containing a fixed Sylow subgroup P of G. This shows M is uniquely determined by P as $N_G(J(P))$. Furthermore, since every Sylow p-subgroup P^* of M is Sylow in G, likewise M is uniquely characterized as $M = N_G(J(P^*))$. We record this observation as

$$M \textit{ is the unique maximal subgroup containing } P^*\textit{, for every } P^* \in Syl_p(M). \tag{3.5}$$

[Another way of looking at this—which *does* require the specific properties of the J-subgroup (see Subsection 3.1)—is that since $J(P) \trianglelefteq M$, we have $J(P) \leq M_p$; this forces $J(P) = J(M_p)$, and the latter subgroup is "intrinsic" to M (characteristic in M, not just in P). Since $M_p \leq P^*$ for every P^* as above, $J(M_p) = J(P^*)$ as well. Alternatively, $J(P)^g = J(P^g)$ for all g in G, so if $J(P) \trianglelefteq M$, then $J(P) = J(P^*)$ by conjugacy of Sylow p-subgroups in M.]

We next show

$$N_G(P_0) \leq M \textit{ for every nontrivial } p\textit{-subgroup } P_0 \textit{ of } M. \tag{3.6}$$

[Recall that the subgroups $N_G(P_0)$ are called *p-local subgroups of G*; so (3.6) says that M contains all p-locals for its nontrivial p-subgroups. In modern parlance M is said to be *strongly p-embedded* in G.]

Let P_0 be a counterexample to (3.6) with $|N_G(P_0) \cap M|_p$ maximal, and let $N = N_G(P_0)$, so $N \not\leq M$. Let P_1 be a Sylow p-subgroup of $N_M(P_0) = N \cap M$, so $|P_1| = |N \cap M|_p$. By normality of P_0 in N we get $P_0 \leq P_1$. Replacing P by an M-conjugate if necessary, we may assume $P_1 \leq P$; so $P_1 = P \cap N$. Since $N \not\leq M$, it follows from (3.5) that $P_1 \neq P$. Since normalizers "grow" in p-groups and P_0 is proper in P, we have $P_0 < P_1$. Let $P_2 := N_P(P_1)$, so since $P_1 < P$, likewise $P_1 < P_2$. [It may help the reader to draw a partial lattice of all the subgroups we've just defined.]

The first step to proving (3.6) is:

$$P_1 = P \cap N \textit{ is a Sylow } p\textit{-subgroup of } N. \tag{3.6a}$$

To see this intermediate step: Since $P_1 < P_2 \leq M \cap N_G(P_1)$, it follows from the maximality condition that defined P_0 that $N_G(P_1) \leq M$. If P_1 is not Sylow in N, then again since normalizers "grow" in a Sylow p-subgroup of N containing P_1, it follows that $|N_N(P_1)|_p > |P_1|$; but $N_N(P_1)$ is contained in $N \cap M$ contrary to P_1 being Sylow in $N \cap M$. This contradiction proves (3.6a).

Continuing the proof of (3.6), we next show

$$J(P_1) \trianglelefteq N. \tag{3.6b}$$

We do this by verifying that $K = N$ satisfies the hypotheses of Theorem 3.1 (applied with P_1 as a Sylow p-subgroup of K). For Hypothesis (1): Since $Z(P) \leq N_G(P_0) = N$, by (3.2) we get $O_q(N) = 1$. For Hypothesis (2): Since $Z(P) \leq Z(P_1)$, (3.3) says $C_N(t) = P_1$, for any element t of order p in $Z(P) \leq Z(P_1)$, as needed to verify the (stronger) Hypotheses (2*). Theorem 3.1 now gives (3.6b).

For the final step in the proof of (3.6): Recall that $P_1 < N_P(P_1) = P_2$. Thus $J(P_1)$ char $P_1 \trianglelefteq P_2$, so by "transitivity of normality for characteristic subgroups," $J(P_1) \trianglelefteq P_2$. Thus by (3.6b),

$$P_1 < P_2 \leq N_G(J(P_1)) \cap M \qquad \textit{and} \qquad N \leq N_G(J(P_1)). \tag{3.6c}$$

The second containment implies $N_G(J(P_1)) \not\leq M$, hence altogether (3.6c) says $J(P_1)$ violates the maximality condition that defined P_0. This contradiction establishes (3.6).

We now easily finish the proof of Theorem C: Break the symmetry between p and q by choosing notation so that $p^a > q^b$. The final contradiction comes from showing that

$$M \textit{ contains every Sylow } p\textit{-subgroup of } G \tag{3.7}$$

since then $\langle\, Syl_p(G) \,\rangle$ is a nontrivial proper normal subgroup of G. Let P^* be any Sylow p-subgroup of G and let $P_0 = P^* \cap M$. By the above choice of notation, since PP^* is a subset of G (not necessarily a subgroup), the usual order formula gives

$$p^a p^a > p^a q^b = |G| \geq |PP^*| = \frac{|P||P^*|}{|P \cap P^*|} = \frac{p^a p^a}{|P \cap P^*|}.$$

This forces $|P \cap P^*| > 1$; and since $P \leq M$ we get $P_0 \neq 1$. If $P_0 = P^*$, then $P^* \leq M$ as claimed in (3.7). Otherwise, $P_0 < P^*$. Then by (3.6), $N_G(P_0) \leq M$. Since normalizers "grow" in p-groups, $P_0 < N_{P^*}(P_0) \leq P^* \cap M = P_0$, a contradiction. This proves (3.7) and so completes the proof of Theorem C.

[We've come full-circle: The final paragraph in the proof of Theorem C contains the essential ingredients for the solution to the Exercise 5 on page 1 that instigated these notes.]

Section 3.1 — The Thompson Factorization Theorem.

We begin by reviewing basic facts about abelian p-groups and their automorphism groups, for p any prime. (Readers may wish to review Section 4.4 of [DF] first too.) Let A be a nontrivial finite abelian p-group. By the Fundamental Theorem of Finite Abelian Groups (proved in Section 6.1 of [DF]), A has a unique decomposition as

$$A \cong Z_{p^{\alpha_1}} \times Z_{p^{\alpha_2}} \times \cdots \times Z_{p^{\alpha_r}}, \quad \text{where } 0 < \alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_r. \tag{$*$}$$

The invariant r is called the *rank* of A—it is characterized as the *minimum number of generators of* A and is denoted as $m(A)$. We say A is *elementary abelian* if all $\alpha_i = 1$ above, in which case

A is the direct product of r copies of Z_p, and is denoted as E_{p^r}. Each A as in $(*)$ has a unique elementary abelian subgroup, A_0, of maximal rank (in modern notation A_0 is denoted by $\Omega_1(A)$):

$$A_0 = \{x \in A \mid x^p = 1\} = \Omega_1(A).$$

(We may think of A_0 as "being at the bottom of A".) It is easy to see that $A_0 \cong E_{p^r}$ and $m(A_0) = m(A)$.

Next assume $A = A_0$ is elementary abelian of rank r. If we write A in additive notation then we may view A as a vector space over $\mathbb{F}_p$, where $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is the finite field of p-elements. From this perspective $m(A)$ equals the vector space dimension of A—any minimal set of generators of A is an $\mathbb{F}_p$-basis of A. The subgroups B of A are vector subspaces, and the dimension of B is its rank too. Of special utility is the dimension formulas for A that say

$$m(B + C) = m(B) + m(C) - m(B \cap C), \quad \textit{for any subgroups } B,\ C \textit{ of } A. \tag{$**$}$$

(This is an immediate consequence of the general *Diamond Isomorphism Theorem* for groups.) A subspace of A of dimension $r - 1$ is called a *hyperplane of* A; so hyperplanes are just the subgroups of index p in A. Of special interest to our proof is the trivial consequence of $(**)$:

$$m(B_1 \cap B_2) = r - 2, \quad \textit{for any distinct hyperplanes } B_1 \textit{ and } B_2 \textit{ of } A.$$

In this notation we may rewrite SOL 4* as: *for any distinct primes* p, q,

$$\begin{gathered}\textit{if } F \textit{ is a } q\textit{-group normalized by any nontrivial elementary abelian } p\textit{-group } A,\\ \textit{then} \quad F = \langle\, C_F(B) \mid B \textit{ is a hyperplane of } A \,\rangle.\end{gathered} \tag{SOL 4*}$$

(We allow the trivial case when $|A| = p$ too.)

Assume $A \cong E_{p^r}$ is a subgroup of a larger group G. If a subgroup H of G acts by conjugation on A (normalizes A), then this action is $\mathbb{F}_p$-linear, i.e., H acts as linear transformations on A; so the elements of H can be represented by matrices with entries from $\mathbb{F}_p$. If $\mathrm{Aut}(A)$ denotes the collection of all group automorphisms of A, then $\mathrm{Aut}(A) = GL(A) \cong GL_r(\mathbb{F}_p)$. I've included a compendium of results from linear algebra and linear groups at the end of this section — it's way more information than we actually need, but results are stated in general form for greater clarity and comprehensiveness.

With this review in mind, we now define the *Thompson subgroup* of any (finite) p-group P. We do this by *modifying* the version stated as Exercise 20, Section 4.4 in [DF]. The version below has been altered from the book by the following changes:

(i) The functions d and m below have been interchanged from their book definitions. (The definitions given above are the ones used most commonly in the literature, including in the original [Th] and in [Asc].)

(ii) The definition of $J(P)$ is only given for p-groups. (I do not know of any instances where the J-subgroup is used for non-p-groups.)

(iii) $J(P)$ is defined in terms of *elementary* abelian p-subgroups, rather than arbitrary abelian p-subgroups of P. (This also necessitates changing the "answer" for $P = Q_8$ in part (c).)

The book definition of the J-subgroup is the version Thompson originally formulated in [Th],[1] and sometimes the one below is distinguished from it by calling it $J_e(P)$ (the subscript "e" being to signal "elementary subgroups generating"). However, the version below (without the subscript e) is

[1] In his original paper, Thompson used T instead of P for the p-group in his definition. I was once at a conference where, in a talk he was giving, John stated that he did *not* intend John Thompson to be the eponym for $J(T)$!

now much more prevalent in the literature—for example, in Aschbacher's book [Asc]. The definition of a J-subgroup in [Gor]—due to George Glauberman—is different from both of these(!), but is rarely used. Here is the (modified) [DF] Exercise:

20*. Let p be a prime and let P be a finite p-group. For any abelian subgroup A of P let $m(A)$ be the minimum number of generators of A (called the *rank* of A). [So, for example, $m(A)) = 1$ if and only if A is a nontrivial cyclic group.] Let $d(P)$ be the maximum of the integers $m(A)$ as A runs over all *abelian* subgroups of P. [So for example, $d(Q_8) = 1$ and $d(D_8) = 2$.] Let $\mathcal{A}(P)$ be the collection of all *elementary abelian* subgroups of P of maximal rank:

$$\mathcal{A}(P) = \{A \mid A \text{ is an elementary abelian subgroup of } P \text{ with } m(A) = d(P)\},$$
$$\text{and define} \quad J(P) = \langle\, \mathcal{A}(P) \,\rangle.$$

$J(P)$ is called the *Thompson subgroup* of P. (Note that $J(P) \neq 1$ if $P \neq 1$.)

(a) Prove that $J(P)$ is a characteristic subgroup of P.

(b) For each of the following 2-groups P list all abelian subgroups A of P that satisfy $m(A) = d(P)$, and state which of these is *elementary* abelian:
$P = Q_8$, D_8, D_{16} and QD_{16} (where QD_{16} is the quasidihedral group of order 16 defined in Exercise 11 of Section 2.5). [You may use the lattices of subgroups for these groups in Section 2.5.]

(c) Show that $J(Q_8) = \langle\, -1 \,\rangle$, $J(D_8) = D_8$, $J(D_{16}) = D_{16}$ and $J(QD_{16})$ is a dihedral subgroup of order 8 in QD_{16}.

(d) Prove that if $H \leq P$ and $J(P)$ is contained in H, then $J(P) = J(H)$.

(e) Deduce that if H is a subgroup of P (not necessarily normal) and $J(H)$ is contained in some subgroup K of H with $K \trianglelefteq G$, then $J(H) \trianglelefteq P$.

See also Exercise 1 at the end of this section for another family of p-groups where the J-subgroup is easily calculated.

We now state the main theorem of this subsection.

Theorem 3.1. *(Thompson)* Let K be a finite solvable group, let p be a prime dividing $|K|$, let P be a Sylow p-subgroup of K, and let $Z = \Omega_1(Z(P))$ (the group generated by all elements of order p in $Z(P)$). Assume the following:

(1) $O_{p'}(K) = 1$, and

(2) $C_K(Z) = P$.

Then one of the following holds:

(i) $p = 2$ with $2^3 3 \,\big|\, |K|$,

(ii) $p = 3$ with $2^2 3^3 \,\big|\, |K|$, or

(iii) $J(P) \trianglelefteq K$.

Theorem 3.1 is a special case of the *Thompson Factorization Theorem*, which removes hypotheses (1) and (2) and concludes more generally that either K *factors* as $K = N_K(J(P))C_K(Z)O_{p'}(K)$ (as in conclusion (iii)) or K has some specifically defined normal subgroups (isomorphic to direct products of $SL_2(p)$'s when $p = 2$ or 3); in the latter conclusion $6 \,\big|\, |K|$ automatically holds—which is what we need for our Theorem C (see [Asc], Section 32). Our proof is closely modeled on arguments in [Th], but because our hypotheses are more restricted—but still sufficient for Theorem C—it can take some "shortcuts" from the lines of reasoning in both [Th] and [Asc]. In

particular, it avoids invoking the three "overhead" facts cited at the outset of [Th] (although one of these is essentially replaced by SOL 4*).

In the proof of Theorem C we use the observation that hypothesis (2) holds whenever we have the (stronger) condition:

(2*) $C(t) = P$, for some element t of order p in $Z(P)$.

((2*) $\implies$ (2)) because $P \leq C_K(Z) \leq C_K(t)$.)

Careful reading shows that conclusions (i) and (ii) can be removed if instead we add the hypothesis that the Sylow 2-subgroups of K are abelian: The divisibility conclusions only emerge at the very end of the proof, where this substitution may be made. See also Exercises 4 and 5 at the end of this section for additional insights.

Proof of Thompson: By way of contradiction let K satisfy the hypotheses and be of minimal order with respect to the property that $J(P)$ is not normal in K. [Note that as we replace K by other counterexamples K_0 satisfying the hypotheses, the Sylow p-subgroup of K_0, and therefore its J-subgroup, may change; so, built in to this minimality is the changing of these J-subgroups too.] Let $K_p = O_p(K)$. By hypothesis (1) and SOL 1 and SOL 2 we have $K_p \neq 1$ and

$$C_K(K_p) = Z(K_p) \quad \textit{and so} \quad Z \leq K_p. \tag{3.1.1}$$

Let $V = \Omega_1(Z(K_p)) = \{x \in Z(K_p) \mid x^p = 1\}$. Thus V is an elementary abelian p-group on which K acts by conjugation. We argue that the kernel of this action is K_p:

$$C_K(V) = K_p \quad \textit{so} \quad \overline{K} := K/K_p \textit{ acts faithfully on } V. \tag{3.1.2}$$

This is because by (3.1.1), $Z \leq V$, so by hypothesis $C_K(V) \leq C_K(Z) = P$. Thus $C_K(V)$ is a normal p-subgroup of K, hence is contained in $O_p(K) = K_p$; by definition of V the reverse containment holds. This proves (3.1.2).

We next argue that

$$\begin{gathered} K = AK_pQ, \quad \textit{for some } A \in \mathcal{A}(P) \textit{ with } A \not\leq K_p, \textit{ where} \\ \overline{Q} \textit{ is a normal } q\textit{-subgroup of } \overline{K} \textit{ acted on nontrivially by } \overline{A}, \textit{ for some prime } q \neq p. \end{gathered} \tag{3.1.3}$$

To prove this first observe that by Exercise 20*(d) above, $J(P) \not\leq K_p$. Thus there must be some $A \in \mathcal{A}(P)$ with $A \not\leq K_p$ — this is the A we want.

[One way of proceeding is to use Hall's Theorems on the existence of $\{p, q\}$-Hall subgroups in solvable groups, given as Exercise 33, Section 6.1 of [DF] (not in the Appendix). We choose a slightly more efficient method that invokes the generalization of SOL 2 alluded to in Section 2.]

First quote Exercise 34* in Section 6.1 of the Appendix: Let $F(\overline{K})$ be the *Fitting subgroup* of the solvable group $\overline{K}$. Since $O_p(\overline{K}) = \overline{1}$, $F(\overline{K})$ is the product of the $O_q(\overline{K})$ as q runs over all primes $\neq p$. Since A is a p-group, part (c) of that exercise says $\overline{A}$ acts faithfully on $F(\overline{K})$, hence it must act nontrivially (but not necessarily faithfully) on $O_q(\overline{K})$ for some prime $q \neq p$. Fix such a q. Let Q be a Sylow q-subgroup of the complete preimage of $O_q(\overline{K})$ in K; so K_pQ is that complete preimage, and is normal in K. Thus $K_0 := A(K_pQ)$ is a subgroup of K. Note that K_0 is a $\{p, q\}$-group with $P_0 := AK_p \in Syl_p(K_0)$.

We verify the hypotheses of Theorem 3.1 for K_0: Hypothesis (2) holds for K_0 since $Z \leq K_p \leq P_0$, so $Z \leq \Omega_1(Z(P_0))$; and hence we get $C_{K_0}(\Omega_1(Z(P_0))) \leq C_{K_0}(Z) = P_0$, which implies (2). Hypothesis (1) holds for K_0 because $Z \leq K_p \leq O_p(K_0)$ and $O_p(K_0)$ centralizes $O_q(K_0)$; and so because Hypothesis (2) holds for K, it forces $O_q(K_0) = 1$. This checks both hypotheses. We next show K_0 is a counterexample.

Since $m(A) = d(P)$ and $d(P_0) \leq d(P)$, we must have $m(A) = d(P_0)$ and so $A \in \mathcal{A}(P_0)$; hence $A \leq J(P_0)$. Furthermore, since $\overline{A}$ acts nontrivially on $\overline{Q}$, we cannot have $A \leq O_p(K_0)$; so it follows that $J(P_0)$ is not normal in K_0. This shows K_0 is a counterexample to Theorem 3.1, so by minimality of K we get $K = K_0$ and so (3.1.3) holds.

[Note: We were *not* asserting that $J(P) = J(P_0)$, nor did we claim $O_p(K_0) = K_p$, but only that $J(P_0)$ is not normal in K_0 because of the nontrivial action of $\overline{A}$ on $\overline{Q}$.]

Next we prove

$$|\overline{A}| = |A \,:\, A \cap K_p| = p. \tag{3.1.4}$$

To see this: By SOL 4*, $\overline{Q}$ is generated by the collection of subgroups $C_{\overline{Q}}(\overline{B})$ as $\overline{B}$ runs over all hyperplanes of $\overline{A}$. Each of these centralizers is stable under conjugation by $\overline{A}$. Since $\overline{A}$ acts nontrivially on $\overline{Q}$, there must be *some* hyperplane $\overline{B}_1$ such that $\overline{A}$ acts nontrivially on $C_{\overline{Q}}(\overline{B_1})$. Let $\overline{Q_1} = C_{\overline{Q}}(\overline{B_1})$, and let Q_1 be the subgroup of Q that maps to $\overline{Q_1}$ under "bar". Let $K_1 = AK_pQ_1$. As before since A normalizes K_pQ_1, we see that K_1 is a subgroup of K. Now use the exact same reasoning as in the proof of (3.1.3) to show that K_1 satisfies the hypotheses of the theorem and is also a counterexample, hence by minimality $K_1 = K$ (details are left to the reader). Consequently we get $Q_1 = Q$. By construction, $\overline{B_1}$ now centralizes $\overline{Q} = O_q(\overline{K})$; so by SOL 2 (invoked with p and q interchanged) we get $\overline{B_1} = \overline{1}$. This establishes (3.1.4).

Henceforth let $B = A \cap K_p$, so B is a hyperplane of A and $A = B \times \langle\, a \,\rangle$, where we now fix $a \in A - B$. By (3.1.3) and (3.1.4), $\langle\, \overline{a} \,\rangle$ is a Sylow p-subgroup of $\overline{K}$. Since $O_p(\overline{K}) = \overline{1}$, there must be a second Sylow p-subgroup, $\langle\, \overline{a^g} \,\rangle$, in $\overline{K}$. Fix such $g \in K$. Then $\langle\, \overline{a}, \overline{a^g} \,\rangle$ has more than one Sylow p-subgroup, so it follows that

$$H := \langle\, a, a^g \,\rangle \text{ is not a } p\text{-group, for some fixed } g \in K. \tag{3.1.5}$$

[Note that we did *not* quote the Baer–Suzuki Theorem to assert (3.1.5)! In what follows, keep in mind that $\overline{a}$ and a act the same way on V, so we drop the "bar" when considering the action of a.]

The nub of the proof is the next point, where the specific nature of the J-subgroup comes into focus:

$$a \text{ centralizes a hyperplane of } V. \tag{3.1.6}$$

To see this let $m(A) = r = d(P)$, so $m(B) = r - 1$. Since $B \leq K_p$ and $V \leq Z(K_p)$, the subgroup generated by B and V is both abelian and generated by elements of order p; hence BV, written additively as $B + V$, is elementary abelian. Since $B \leq B + V$ and since every elementary abelian subgroup of P has rank $\leq r$, we must have

$$r - 1 = m(B) \leq m(B + V) \leq r.$$

Since a does not centralize V by (3.1.2), but it does centralize B, we must have $B + V \neq B$. This implies $m(B + V) = r$ and by $(**)$, $B \cap V$ is a hyperplane of V. This implies (3.1.6).

Since a^g is a conjugate of a, it too centralizes a hyperplane of V. From $(**)$ we get

$$H \text{ centralizes the subspace } W := C_V(a) \cap C_V(a^g) \text{ of } V \text{ of dimension} \geq \dim V - 2. \tag{3.1.7}$$

We next show that

$$\widetilde{V} := V/W \cong E_{p^2} \text{ is 2-dimensional} \quad \text{and} \quad a \text{ acts nontrivially on } \widetilde{V}. \tag{3.1.8}$$

By (3.1.7), $\widetilde{V}$ is a space of dimension ≤ 2. If H also centralizes $\widetilde{V}$, then by Exercise 3 at the end of this section, all elements of order q in H centralize V, a contradiction (since by (3.1.5), H contains

nontrivial q-elements, all of which act faithfully on V). This proves a must act nontrivially on $\widetilde{V}$. Hence $\widetilde{V}$ cannot be one-dimensional (i.e., of order p), since in that case a (and a^g) would act trivially on $\widetilde{V}$ (as $\mathrm{Aut}(Z_p)$ has order $p-1$); so $\widetilde{V} \cong E_{p^2}$ is 2-dimensional, as needed for (3.1.8).

[Remark: At this point it might be worthwhile to review the compendium of results from linear groups at the end of this subsection.]

Thus a permutes the $p+1$ one-dimensional subspaces (the lines) of $\widetilde{V}$ — call this set $\mathcal{L}$. If a acts trivially on $\mathcal{L}$ then so too does a^g. In this case let C be any hyperplane of V with $0 \leq W < C < V$; so $C/W \in \mathcal{L}$ is fixed by both a and a^g. Since V/C and C/W are both one-dimensional, both a and a^g act trivially on the successive quotients in the chain, and so again by Exercise 3 the elements of order q in H centralize V, a contradiction.

Since a acts nontrivially on $\mathcal{L}$, it permutes it as a p-cycle and a 1-cycle. Let C be the hyperplane of V with $W < C < V$ and C/W the element of $\mathcal{L}$ fixed by a (the 1-cycle orbit). If a^g also fixes the line C/W, then $\langle\, a, a^g \,\rangle$ acts trivially on successive quotients in the same chain as the previous paragraph, a contradiction. This proves a^g must move the element C/W of $\mathcal{L}$. This is enough to ensure

$$H = \langle\, a, a^g \,\rangle \text{ acts transitively on the set } \mathcal{L} := \{\, p+1 \text{ lines in } \widetilde{V} \,\}. \tag{3.1.9}$$

The "orbit-stabilizer theorem" (Proposition 2, Section 4.1 of [DF]) then gives that $p+1$ divides $|H|$. Thus the order of K is divisible by $|\widetilde{V}| \cdot |a| \cdot (p+1) = p^3(p+1)$.

[Note that if we were only interested in proving Theorem 3.1 for odd order groups, we could stop here; but finishing the general case is easily done with only a bit of "[DF]–overhead" needed.]

If $p = 2$, then conclusion (i) holds. If $p = 3$, then conclusion (ii) holds.

Assume $p \geq 5$. Let H_0 be the kernel of the action of H on $\mathcal{L}$, and let $\widehat{H} = H/H_0$, so $\widehat{H}$ acts faithfully on $\mathcal{L}$. Since $\widehat{H}$ is generated by two elements of order p, by Exercise 6(a) below it is isomorphic to a subgroup of $PSL_2(p)$. Of course $\widehat{H}$ is also a $\{p,q\}$-group. Since $p+1 \,\big|\, |\widehat{H}|$ and $(p, p+1) = 1$, we must have

$$p+1 = q^c, \quad \text{for some } c \geq 2.$$

Thus $p = q^c - 1$ is divisible by $q-1$ and so $q = 2$.

Next, by (3.1.9) together with the fact that $\langle\, a \,\rangle$ has orbits of size p and 1 on $\mathcal{L}$, we get

$$\widehat{H} \text{ acts doubly transitively on } \mathcal{L}. \tag{3.1.10}$$

(See Exercises 7 to 9 in Section 4.1 of [DF]—in the Appendix—for relevant definitions and properties of permutation groups.) Let $\widehat{N}$ be a minimal normal subgroup of the solvable group $\widehat{H}$, so $\widehat{N}$ is elementary abelian. By the Exercise 9(c)* of Section 4.1, display (3.1.10) implies

$$\widehat{N} \text{ acts transitively on } \mathcal{L}, \quad \text{so} \quad 2^c = p+1 \,\big|\, |\widehat{N}|.$$

Thus $\widehat{N}$ is an elementary abelian 2-group and $m(\widehat{N}) \geq c$. Since $5 \leq p = 2^c - 1$ we must have $c \geq 3$. By Exercise 6(c) below, however, $m(\widehat{A}) \leq 2$ for every elementary abelian 2-subgroup $\widehat{A}$ of $PSL_2(p)$, a contradiction. This completes the proof of Theorem 3.1.

[An alternative way of proceeding after (3.1.8) is to show $\overline{H} \cong SL_2(p)$ and then (independently) show $SL_2(p)$ is nonsolvable for $p \geq 5$. That approach seems less consonant with our development.]

Outline of a proof of SOL 4*.

For p and q any distinct primes, the statement SOL 4* is:

$$\begin{array}{c} \textit{if } F \textit{ is a } q\textit{-group normalized by any nontrivial elementary abelian } p\textit{-group } A, \\ \textit{then} \quad F = \langle\, C_F(B) \mid B \leq A \text{ with } |A : B| = p \,\rangle. \end{array} \tag{SOL 4*}$$

Proofs of this ultimately rely on the following:

$$\textit{Any finite abelian subgroup of the multiplicative group of a field is cyclic,} \tag{$***$}$$

found in Section 9.5 of [DF] as Proposition 18. This is the essential underpinning of *Schur's Lemma*, which is the specific result we need.

[The variant of Schur's Lemma for group algebras over the complex numbers is Exercise 17 in Section 18.1 of [DF] (listed in the Appendix). We need the corresponding version for group algebras over certain finite fields.]

We sketch how this works. Let A, F be a minimal counterexample with $|F|$ minimal and, subject to this, with $|A|$ minimal (so A is clearly not cyclic). First use the second approach hint to a proof of SOL 4 outlined at the end of Section 2: Show $F/\Phi(F)$ is also a counterexample, where $\Phi(F)$ is the Frattini subgroup of F. By minimality then $\Phi(F) = 1$, i.e.,

$$F \textit{ is an elementary abelian } q\textit{-group } E_{q^n}\textit{, for some } n \geq 1.$$

Now write F in additive form, and to emphasize this perspective *use V in place of F*—thus V is a vector space over the finite field $\mathbb{F}_q$, where $q \neq p$ (this is *not* the "V" in Subsection 3.1).

By minimality of A and V, using Exercise 20(b) of Section 6.1 (with p, q interchanged in the application) argue that

$$\begin{array}{c} A \textit{ acts faithfully on } V, \\ \langle\, C_V(B) \mid B \leq A \textit{ with } |A : B| = p \,\rangle = 0, \textit{ and} \\ \textit{there is no nontrivial proper subspace of } V \textit{ that is normalized by } A. \end{array} \tag{$\dagger$}$$

Let $S = \mathbb{F}_q[A]$ be the group ring of A with coefficients from $\mathbb{F}_q$, as described in Section 7.2 of [DF] (where it is simply denoted by $\mathbb{F}_q A$). Note that S is a commutative, finite ring with 1. The action of A by conjugation makes V into an $\mathbb{F}_q[A]$-module, i.e., an S-module, as described in detail in Section 18.1. The third line in ($\dagger$) is, by definition, the statement that

$$V \textit{ is an irreducible } S\textit{-module on which } A \textit{ acts as } S\textit{-module endomorphisms.}$$

Now invoke the elementary version of Schur's Lemma stated in Exercise 11, Section 10.3 of [DF] (in the Appendix) to obtain:

$$\mathrm{End}_S(V) \textit{ is a division ring.}$$

With the group operation in A written (as usual) multiplicatively, the group product of two elements of A is their composition as endomorphisms of the S-module V (and multiplication in the ring $\mathrm{End}(V)$ is composition of endomorphisms—see Section 10.2 of [DF]). So each element of A is an *invertible* endomorphism of V since the group A contains group inverses. (Alternatively, since $\mathrm{End}_S(V)$ is a division ring, every nonzero element in it is invertible!) Thus A is (represented faithfully as) a finite subgroup of the multiplicative group of the division ring $\mathrm{End}_S(V)$. Since multiplication of elements in A is commutative, the subring generated by A and $\mathbb{F}_q$ in $\mathrm{End}_S(V)$ is a field. By ($***$), A is cyclic, a contradiction. This proves SOL 4*.

Another way of approaching SOL 4* is to use the result that, because there are p distinct p^{th} roots of unity in some extension field L of $\mathbb{F}_q$, each element of A can be represented as a diagonal matrix with entries from L ($q \neq p$ is required for this). Since A is abelian, it follows by induction that the elements of A can be *simultaneously* diagonalized over L. This easily shows that $V \otimes_{\mathbb{F}_q} L$ is generated by centralizers of hyperplanes B of A. One can use "descent arguments" to then show the same generation is true for V over $\mathbb{F}_q$ (although V does not decompose into eigenspaces for elements of A over $\mathbb{F}_q$). This "diagonalization method", ultimately essentially relies on $(***)$ too.

If $p \mid q-1$ we may take $L = \mathbb{F}_q$, and the "descent" step is not required: A is represented by diagonal matrices with entries from $\mathbb{F}_q$. This is part of the reason that the original SOL 4 has easier proofs: 2 always divides $q-1$; and the diagonalization method is explicitly describable.

Review of Linear Groups.

This is a review of some results from basic linear algebra and linear groups. The facts herein are either already in Sections 11.1 to 11.4 of [DF], or are easy exercises from that material. The special case when the vector space is of dimension 2 and the field is the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ of p elements are what is needed in these notes; but proofs of the general results are the same. Let F be any field and let V be a vector space over F of finite dimension $n \geq 1$. Let $F^\times$ denote the multiplicative group of all nonzero elements of F.

Let $GL(V)$ be the group of all nonsingular linear transformations from V to itself — the *general linear group*. Let $GL_n(F)$ be all $n \times n$ invertible matrices, which is a group under matrix multiplication. (If F is the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ for p a prime, use $GL_n(p)$ to denote $GL_n(F)$; and likewise for other linear subgroups.) Then $GL(V) \cong GL_n(F)$, where an isomorphism is given by fixing any basis of V and writing the matrix of each linear transformation with respect to that basis (in the domain and range).

Various subgroups of these general linear groups are of particular interest: The determinant

$$\det : GL_n(F) \longrightarrow F^\times \quad by \quad X \longmapsto \det(X)$$

is a group homomorphism. The determinant of a linear transformation does not depend on the choice of basis representing it as a matrix. Let $SL(V)$ and $SL_n(F)$ be the elements of determinant 1 in the respective general linear groups — the kernel of the determinant map — called the *special linear groups*. Then $SL(V) \trianglelefteq GL(V)$ and $GL(V)/SL(V) \cong F^\times \cong GL_n(F)/SL_n(F)$. Let I denote the identity linear transformation or identity matrix of degree n. A *scalar transformation or matrix* is αI for any $\alpha \in F$. The subgroup of nonzero scalar transformations (or matrices) is a subgroup of $GL(V)$ (respectively $GL_n(F)$) isomorphic to $F^\times$ and is contained in the center of the group. The scalar matrices of determinant 1 are the subgroup $\{\lambda I \mid \lambda^n = 1\}$ of the special linear group. It is an exercise that

the subgroup of nonzero scalars equals the center of the general linear group, and
the subgroup of scalars of determinant 1 equals the center of the special linear group.

If F is a finite field, then the linear groups are finite and their order formulas are given in Section 11.2 of [DF]. In particular, $|GL_2(p)| = (p^2-1)(p^2-p)$ and $|SL_2(p)| = p(p-1)(p+1)$.

The *projective space* over V of degree $n-1$ is the set of all lines or 1-dimensional subspaces in V. We have denoted this by $\mathcal{L}$, but it is also denoted by $\mathbb{P}(V)$ (or $\mathbb{P}_{n-1}(F)$). One easily see that

if F is a finite field, then $|\mathcal{L}| = (|F|^n - 1)/(|F| - 1)$.

Clearly $GL(V)$ acts on $\mathcal{L}$, and the subgroup of scalar transformations acts trivially. It is an exercise to show that

the kernel of the action of $GL(V)$ on $\mathcal{L}$ equals the nonzero scalar matrices,

i.e., $GL(V)/\langle\, \lambda I \mid \lambda \in F^\times \,\rangle$ acts faithfully on $\mathcal{L}$. The latter group is called the *projective general linear group* and is denoted by $PGL(V)$. The *projective special linear group* is denoted $PSL(V) := SL(V)/\{\lambda I \mid \lambda^n = 1\}$ (and denoted $PGL_n(F)$ and $PSL_n(F)$ for the respective matrix groups).

Exercises

1. Let p be an odd prime and let $P = Z_p \wr Z_p$ be the wreath product group of order p^{p+1} (cf., Exercise 23, Section 5.5 of [DF]). Show that $J(P)$ is the unique elementary abelian subgroup of P of rank p. (Check that $Z_2 \wr Z_2 \cong D_8$, so $J(P) = P$ when $p = 2$.)

2. Let K be a solvable group and let p be the smallest prime dividing $|K|$. Prove that if a Sylow p-subgroup of K is cyclic, then K has a normal p-complement.
   (This result is true without the solvability assumption on K, but the general result is usually proved via the transfer homomorphism.)
   [Hint: Reduce to when $O_{p'}(K) = 1$. Use SOL 2 (and the paragraph after it) to show $K = O_p(K)$, where the automorphism group of a cyclic group is derived in Section 4.4 of [DF].]

3. *(Stability groups for co-prime actions)* Let p be a prime and let V be any p-group normalized by a group Q of order prime to p (in some large group containing both V and Q). Assume V contains a chain of subgroups

   $$0 = V_0 \leq V_1 \leq V_2 \leq \cdots \leq V_n = V$$

   such that each V_i is normalized by V and Q with Q acting trivially by conjugation on V_i/V_{i-1} for $1 \leq i \leq n$. Prove that Q acts trivially on all of V.
   (The trivial action hypothesis can alternatively be written as $[V_i, Q] \leq V_{i-1}$ for $1 \leq i \leq n$.)
   [Hint: Reduce by induction to $n = 2$ and Q is a q-group for some prime $q \neq p$. Then use Exercise 20(b) in Section 6.1—see the Appendix—applied with the roles of p and q reversed and its $N = V_1$.]

Remark: In the special case when V is an elementary abelian p-group, you can refine the chain by removing equalities and then adding subspaces between V_i and V_{i+1}, as needed, to make all successive quotients one-dimensional (so V is n-dimensional). Then any vectors e_i chosen with $e_i \in V_i - V_{i-1}$ for $1 \leq i \leq n$ form a basis of V. With respect to such a basis the elements of Q are represented by upper triangular matrices with 1's along the diagonal (unipotent matrices). By order considerations, the subgroup of all unipotent matrices is a Sylow p-subgroup of $GL_n(\mathbb{F}_p)$. Under its action on V the p'-group Q must therefore map to the identity in this p-group, i.e., Q must act trivially. (This is another solution, when V is elementary abelian.) These chains of subspaces are called *flags* in V and a refined chain of length n is a *maximal flag.*

4. Show that $K = S_4$ satisfies all the hypotheses of Theorem 3.1 for $p = 2$. For P a Sylow 2-subgroup of S_4 show $P = J(P)$ and P is *not* normal in S_4. [Hint: See Exercise 20*(c).]
   (Of course $p^3(p+1) = 2^3 \cdot 3$ divides the order of S_4.)

Remark: You can see how $K = S_4$ "emerges" as a prototypical minimal counterexample at the end of the proof, where $V = K_p$ is the unique Klein fourgroup V_4 in the alternating group and the "W subspace" is trivial in this case—this leads to conclusion (i).

5. Let p be any prime and let $H = SL(V) \cong SL_2(p)$ act naturally on the 2-dimensional vector space V over $\mathbb{F}_p$. Let $G = V \rtimes H$ be the semidirect product with respect to this action. Let $P \in Syl_p(G)$. Show that $|P| = p^3$ and that $P = J(P)$. Prove $J(P)$ is *not* normal in G.

Remark: It follows from Theorem 3.1 and this example that $SL_2(p)$ is *not solvable* for all $p \geq 5$. (Solvability is strongly used in the proof of (3.1.3).)
When $p = 2$, $G = K \cong S_4$ as in Exercise 4. When $p = 3$, G is a solvable group of order $2^3 3^3$ with Sylow 2-subgroup of type Q_8. With a tad more work one can actually strengthen conclusion (ii) of Theorem 3.1 to assert that $2^3 3^3 \mid |K|$.

6. Let p be an odd prime, let $G = GL_2(p)$ and let $S = SL_2(p)$ be the general and special linear groups of degree 2 over the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ respectively (where we use without reference the notation and results from the review of linear groups above). Let $\widehat{S} = PSL_2(p)$ be the projective special linear group i.e., S modulo the subgroup of scalars of determinant 1.
   (a) Prove that any subgroup of G generated by elements of order p is contained in S.
   [Hint: $|\mathbb{F}_p^\times| = p - 1$.]
   (b) Prove that $z = -I$ is the *unique* element of order 2 in S.
   [Hint: Use the method in the hints for SOL 4 at the end of Section 2 to show that *any* involution z can be represented by a diagonal matrix with respect to some basis. Then use $\det(z) = 1$ to show z is represented by $-I$, and deduce that the same is true for any basis.]
   (c) Let $T \in Syl_2(S)$ (so $z \in T$ by (b)). Show that $\widehat{T} = T/\langle z \rangle$. Show that $d(\widehat{T}) \leq 2$, where d is the maximum rank of elementary abelian subgroups of $\widehat{T}$ (i.e., show $\widehat{T}$, and hence also $PSL_2(p)$, does not contain a subgroup isomorphic to E_8).
   [Hint: Suppose $\langle z \rangle \leq A \leq T$ with $\widehat{A} \cong E_8$. Show every $x \in A - \langle z \rangle$ has order 4 with $x^2 = z$ and with $\langle x \rangle \trianglelefteq A$. Deduce from normality that $|C_A(x)| > 4$ and so there is some $y \in C_A(x) - \langle x \rangle$. Get a contradiction by showing $|xy| = 2$.]

Remark: It is not hard to prove (by induction) that if T is any 2-group with a unique element z of order 2, then T is either cyclic or generalized quaternion (i.e., Z_{2^m} or Q_{2^m}). Part (c) follows easily from this independent general result, since $T/\langle z \rangle$ is then cyclic or dihedral respectively.

7. Give a different proof of the Baer–Suzuki Theorem for *solvable* groups K, via induction on $|K|$.
   [Hint: Reduce to when $O_p(K) = 1$ and $K = XO_{p'}(K)$ with $X \in Syl_p(K)$.]

Acknowledgments

I am most grateful to Dr. Hy Ginsberg for his careful reading of these notes, and for his helpful clarifications, insights and suggestions. I thank Dr. Dave Dummit for his suggestions on Section 1 as well—they informed the style and content of the other sections too.

References

[AL] J. Alperin and R. Lyons, On conjugacy classes of p-elements, Journal of Algebra, 19(1971), 536–537.

[Asc] M. Aschbacher, *Finite Group Theory*, Cambridge University Press.

[Be] H. Bender, A group theoretic proof of Burnside's p^aq^b-theorem, Math. Z., 126(1972), 327–338.

[DF] D. Dummit and R. Foote, *Abstract Algebra, Third Edition*, Wiley.

[FW] R. Foote and M. Welz, Characterizations of Finite Groups with p-Fusion of Squarefree Type, Bull. Malaysian Mathematical Sciences Soc., Vol. 40, No. 2 (2017), 697–706.

[Gol] D. Goldschmidt, A group-theoretic proof of the p^aq^b-theorem for odd primes, Math. Z., 113(1970), 373–375.

[Gor] D. Gorenstein, *Finite Groups*, Harper & Row or AMS.

[Ma] H. Matsuyama, Solvability of groups of order 2^ap^b, Osaka J. Math., 10(1973), 375–378.

[Th] J.G. Thompson, Normal p-complements for finite groups, J. Algebra, 1(1964), 43–46.

Appendix — Exercises from [DF] and Generalizations

Section 1.2

6. Let x and y be elements of order 2 in any group G. Prove that if $t = xy$ then $tx = xt^{-1}$ (so that if $n = |xy| < \infty$ then x, t satisfy the same relations in G as s, r do in D_{2n}).

Section 1.6

23. Let G be a finite group that possesses an automorphism σ such that $\sigma(g) = g$ if and only if $g = 1$. If σ^2 is the identity map from G to G, prove that σ acts by inversion on G and G is abelian (when $G \neq 1$ such an automorphism σ is called *fixed point free* of order 2). [Show that every element of G can be written in the form $x^{-1}\sigma(x)$ and apply σ to such an expression.]

Section 3.3

9. Let p be a prime and let G be a group of order p^am, where p does not divide m. Assume P is a subgroup of G of order p^a and N is a normal subgroup of G of order p^bn, where p does not divide n. Prove that $|P \cap N| = p^b$ and $|PN/N| = p^{a-b}$. (The subgroup P of G is called a *Sylow p-subgroup* of G. This exercise shows that the intersection of any Sylow p-subgroup of G with a normal subgroup N is a Sylow p-subgroup of N.)

10. Generalize the preceding exercise as follows. A subgroup H of a finite group G is called a *Hall subgroup* of G if its index in G is relatively prime to its order: $(|G : H|, |H|) = 1$. Prove that if H is a Hall subgroup of G and $N \trianglelefteq G$, then $H \cap N$ is a Hall subgroup of N and HN/N is a Hall subgroup of G/N.

Section 4.1

7. Let G be a transitive permutation group on the finite set A. A *block* is a nonempty subset B of A such that for all $\sigma \in G$ either $\sigma(B) = B$ or $\sigma(B) \cap B = \emptyset$ (here $\sigma(B)$ is the set $\{\sigma(b) \mid b \in B\}$).

   (a) Prove that if B is a block containing the element a of A, then the set G_B defined by $G_B = \{\sigma \in G \mid \sigma(B) = B\}$ is a subgroup of G containing G_a.

   (b) Show that if B is a block and $\sigma_1(B), \sigma_2(B), \ldots, \sigma_n(B)$ are all the distinct images of B under the elements of G, then these form a partition of A.

(c) A (transitive) group G on a set A is said to be *primitive* if the only blocks in A are the trivial ones: the sets of size 1 and A itself. Show that S_4 is primitive on $A = \{1, 2, 3, 4\}$. Show that D_8 is not primitive as a permutation group on the four vertices of a square.

(d) Prove that the transitive group G is primitive on A if and only if for each $a \in A$, the only subgroups of G containing G_a are G_a and G (i.e., G_a is a *maximal* subgroup of G, cf. Exercise 16, Section 2.4). [Use part (a).]

8. A transitive permutation group G on a set A is called *doubly transitive* if for any (hence all) $a \in A$ the subgroup G_a is transitive on the set $A - \{a\}$.

(a) Prove that S_n is doubly transitive on $\{1, 2, \ldots, n\}$ for all $n \geq 2$.

(b) Prove that a doubly transitive group is primitive. Deduce that D_8 is not doubly transitive in its action on the 4 vertices of a square.

9. Assume G [any group] acts transitively on the finite set A and let H be a normal subgroup of G. Let $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_r$ be the distinct orbits of H on A.

(a) Prove that G permutes the sets $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_r$ in the sense that for each $g \in G$ and each $i \in \{1, \ldots, r\}$ there is a j such that $g\mathcal{O}_i = \mathcal{O}_j$, where $g\mathcal{O} = \{g \cdot a \mid a \in \mathcal{O}\}$ (i.e., in the notation of Exercise 7 the sets $\mathcal{O}_1, \ldots, \mathcal{O}_r$ are *blocks*). Prove that G is transitive on $\{\mathcal{O}_1, \ldots, \mathcal{O}_r\}$. Deduce that all orbits of H on A have the same cardinality.

(b) Prove that a doubly transitive group is primitive.

(c)* *(added to book)* Deduce that a nontrivial normal subgroup of a doubly transitive permutation group is transitive.

Section 4.5

37. Let R be any normal p-subgroup of G (where G is any finite group).

(a) Prove that R is contained in every Sylow p-subgroup of G.

(b) If S is another normal p-subgroup of G, prove that RS is also a normal p-subgroup of G.

(c) The subgroup $O_p(G)$ is defined to be the group generated by all normal p-subgroups of G. Prove that $O_p(G)$ is the unique largest normal p-subgroup of G and $O_p(G)$ equals the intersection of all Sylow p-subgroups of G.

(d) Let $\overline{G} = G/O_p(G)$. Prove that $O_p(\overline{G}) = \overline{1}$ (i.e., $\overline{G}$ has no nontrivial normal p-subgroup).

Generalize the preceding exercise as follows (where G is any finite group):

37*. Let π be any set of primes (possibly infinite). Recall that a *π-group* is any group whose order is divisible by only primes in π. Let R be a normal π-subgroup of G.

(a) If S is another normal π-subgroup of G, prove that RS is also a normal π-subgroup of G.

(b) The subgroup $O_\pi(G)$ is defined to be the group generated by all normal π-subgroups of G. Prove that $O_\pi(G)$ is the unique largest normal π-subgroup of G.

(c) Let $\overline{G} = G/O_\pi(G)$. Prove that $O_\pi(\overline{G}) = \overline{1}$ (i.e., $\overline{G}$ has no nontrivial normal π-subgroup).

Simplify notation, as in Exercise 37, by using $O_p(G)$ to denote $O_{\{p\}}(G)$.

In general, for any set of primes π let π' be the set of all primes not in π, and so $O_{\pi'}(G)$ is the largest normal subgroup of G whose order is relatively prime to all primes in π. If $\pi = \{p\}$, simplify notation by using $O_{p'}(G)$ to denote $O_{\pi'}(G)$.

In the special case when $|G| = p^a q^b$ for p, q distinct primes, $O_{p'}(G) = O_q(G)$ (and vice versa).

(d) Prove that $O_\pi(G)$ and $O_{\pi'}(G)$ commute (elementwise). [Hint: Consider $[O_\pi(G), O_{\pi'}(G)]$.]

Section 6.1

20. Let p be a prime, let P be a p-subgroup of the finite group G, let N be a normal subgroup of G whose order is relatively prime to p and let $\overline{G} = G/N$. Prove the following:

    (a) $N_{\overline{G}}(\overline{P}) = \overline{N_G(P)}$ [Use Frattini's Argument.]

    (b) $C_{\overline{G}}(\overline{P}) = \overline{C_G(P)}$. [Use part (a).]

Comment: For any group G the *Frattini subgroup* of G (denoted by $\Phi(G)$) is defined to be the intersection of all the maximal subgroups of G (if G has no maximal subgroups, set $\Phi(G) = G$).

26. Let p be a prime, let P be a finite p-group and let $\overline{P} = P/\Phi(P)$.

    (a) Prove that $\overline{P}$ is an elementary abelian p-group. [Show that $P' \leq \Phi(P)$ and that $x^p \in \Phi(P)$ for all $x \in P$.]

    (b) Prove that if N is any normal subgroup of P such that P/N is elementary abelian then $\Phi(P) \leq N$. State this (universal) property in terms of homomorphisms and commutative diagrams.

    (c) Let $\overline{P}$ be elementary abelian of order p^r (by (a)). Deduce from Exercise 24 that if $\overline{x_1}, \overline{x_2}, \ldots, \overline{x_r}$ are any basis for the r-dimensional vector space $\overline{P}$ over $\mathbb{F}_p$ and if x_i is any element of the coset $\overline{x_i}$, then $P = \langle\, x_1, x_2, \ldots, x_r \,\rangle$. Show conversely that if $y_1, y_2, \ldots, y_s$ is any set of generators for P, then $s \geq r$ (you may assume that every minimal generating set for an r-dimensional vector space has r elements, i.e., every basis has r elements). Deduce *Burnside's Basis Theorem*: a set $y_1, \ldots, y_s$ is a minimal generating set for P if and only if $\overline{y_1}, \ldots, \overline{y_s}$ is a basis of $\overline{P} = P/\Phi(P)$. Deduce that any minimal generating set for P has r elements.

    (d) Prove that if $P/\Phi(P)$ is cyclic then P is cyclic. Deduce that if P/P' is cyclic then so is P.

    (e) Let σ be any automorphism of P of prime order q with $q \neq p$. Show that if σ fixes the coset $x\Phi(P)$ then σ fixes some element of this coset (note that since $\Phi(P)$ is characteristic in P every automorphism of P induces an automorphism of $P/\Phi(P)$). [Use the observation that σ acts a permutation of order 1 or q on the p^a elements in the coset $x\Phi(P)$.]

    (f) Use parts (e) and (c) to deduce that every nontrivial automorphism of P of order prime to p induces a nontrivial automorphism on $P/\Phi(P)$. Deduce that any group of automorphisms of P which has order prime to p is isomorphic to a subgroup of $\mathrm{Aut}(\overline{P}) = GL_r(\mathbb{F}_p)$.

31. For any group G a *minimal normal subgroup* is a *nontrivial* normal subgroup M of G such that the only normal subgroups of G which are contained in M are 1 and M. Prove that every minimal normal subgroup of a finite solvable group is an elementary abelian p-group for some prime p. [If M is a minimal normal subgroup of G, consider its characteristic subgroups: M' and $\langle\, x^p \mid x \in M \,\rangle$.]

34. *(Revised from book)* Let p be a prime dividing the order of the finite solvable group G. Assume G has no nontrivial normal subgroup of order prime to p (i.e., $O_{p'}(G) = 1$). Let $P = O_p(G)$ be the largest normal p-subgroup of G (cf. Exercise 37 in Section 4.5. Exercise 31 implies $P \neq 1$). Prove that $C_G(P) \leq P$, i.e., $C_G(P) = Z(P)$.

    [Let $C = C_G(P)$ and by way of contradiction assume $C \not\leq P$. Use Exercise 31 to show that there exists $M \trianglelefteq G$ with $P < M \leq PC$ such that M/P is a q-group, for some prime $q \neq p$ (invoke Exercise 37(d) in Section 4.5 to get $q \neq p$). Let $Q \in Syl_q(M)$. Prove that $Q \leq C$. Deduce that $M = P \times Q$ and consequently that $Q \trianglelefteq G$ to obtain a contradiction.]

The next exercise generalizes Exercise 34 above: It describes the *Fitting subgroup*, $F(G)$, of any finite group G and establishes some of its basic properties. *You can think of this generalization as SOL 2*:* It is analogous to the way Section 4.5, Exercise 37* above generalizes Exercise 37 preceding it.

34*. *(The Fitting Subgroup)* Let G be any finite group.

(a) Prove that if N_1 and N_2 are nilpotent normal subgroups of G, then N_1N_2 is a nilpotent normal subgroup. Deduce that G contains a unique maximal normal nilpotent subgroup—denote it by $F(G)$—called the *Fitting subgroup* of G. (See also Exercises 37 and 37* in Section 4.5.)

(b) Prove that $F(G)$ is the direct product of the subgroups $O_p(G)$ as p runs over all prime divisors of G. Deduce that if $O_{p'}(G) = 1$ then $F(G) = O_p(G)$.

(c) *(The Fitting Subgroup Theorem)* Prove that if K is any finite solvable group, then $C_K(F(K)) \leq F(K)$, i.e., $C_K(F(K)) = Z(F(K))$.
[Use exactly the same reasoning as the hint to Exercise 34 above but with P replaced by $F(K)$, where q is any prime. Derive the contradiction by showing that the resulting M is nilpotent.]

(d) Deduce from (c) that if K is solvable, then $|K| \leq |\mathrm{Aut}(F(K))| \cdot |Z(F(K))|$.

Section 10.3

11. Show that if M_1 and M_2 are irreducible R-modules [where R is any ring with 1], then any nonzero R-module homomorphism from M_1 to M_2 is an isomorphism. Deduce that if M is irreducible then $\mathrm{End}_R(M)$ is a division ring (this result is called *Schur's Lemma*). [Take $M_1 = M_2 = M$ for Schur's Lemma.]

Section 18.1

17. Prove the following variant of Schur's Lemma for complex representations of abelian groups: if G is abelian, any irreducible complex representation, ϕ, of G is of degree 1 and $G/\ker\phi$ is cyclic. [This can be done without recourse to Exercise 14 (in Section 18.1) by using the observation that for any $g \in G$ the eigenspaces of $\phi(g)$ are G-stable. Your proof that ϕ has degree 1 should also work for infinite abelian groups when ϕ has finite degree.]