NILPOTENT GROUPS & FINITE ABELIAN GROUPS

COLTON GRAINGER

8. Assignment due 2018-10-31

8.1. **[1, No. 5.2.8].** Let A be a finite abelian group (written multiplicatively) and let p be a prime. Suppose

$$A^p = \{a^p : a \in A\} \quad \text{and} \quad A_p = \{x : x^p = 1\},$$

so that A^p and A_p are the image and kernel of the pth power map

$$\varphi\colon A \to A \quad \text{such that} \quad \varphi\colon x \mapsto x^p.$$

(a) Prove that $A/A^p \cong A_p$ by showing both are elementary abelian and of the same order.

Proof.[1] Observe $A_p = \ker\varphi$ and $A/A^p = \operatorname{coker}\varphi$. We anticipate a line of argument similar to the rank-nullity theorem from linear algebra.

By the first isomorphism theorem,

$$A/\ker\varphi \cong \operatorname{im}\varphi \quad \text{that is} \quad A/A_p \cong A^p \quad \text{so} \quad |A/A^p| = |A_p|.$$

To see that both A_p and A/A^p are elementary abelian p-groups, check:

- $A_p \ni x$ implies $x^p = 1$.
- $A/A^p \ni xA^p$ implies $(xA^p)^p = x^pA^p = 1 \cdot A^p$.
- Since p is prime, the only element in A_p, A/A^p of order less than p is the identity.

We conclude $A_p \cong A/A^p$ as both are elementary abelian p-groups of the same order, say, both isomorphic to $(\mathbf{F}_p)^n$. □

(b) Prove that the number of subgroups of A of order p equals the number of subgroups of A of index p, by reducing to the case where A is an elementary abelian p-group.

Proof. Since each subgroup of $\ker\varphi = A_p$ is cyclic p, and each subgroup of A of order p is in $\ker\varphi$, our proof reduces to considering the order p subgroups of A_p.

At the same time, we want to show if $H \leqslant A$ is a subgroup of index p, then $A^p \leqslant H$. So let $x \in A^p$. Then $x = a^p$ for some a. Suppose by way of contradiction that $x \notin H$. We must then have $a^p \notin H$, whence $a \notin H$ (by closure). Now the quotient group A/H is of order p and cyclic. With $a \notin H$, we can populate the coset space A/H with $\langle a \rangle = H$. But then

$$H = (aH)^p = a^pH \quad \text{implies} \quad a^p \in H, \quad \text{and so} \quad x \in H,$$

a contradiction. Thus we must have $A^p \leqslant H$. (By line of reasoning similar to the proof of the universal property for the abelianization of a group by quotienting out the commutator) the third isomorphism theorem implies

$$A/H \cong (A/A^p)/(H/A^p).$$

Date: 2018-10-28.

Compiled: 2018-10-31.

[1]See also https://math.stackexchange.com/questions/413470/, https://math.stackexchange.com/questions/142589/.

So just as with the kernel A_p, with the cokernel A/A_p it suffices to consider the number of index p subgroups in A/A^p to find the number of index p subgroups in A.

Now $A_p \cong A/A^p \cong (\mathbf{F}_p)^n$. We need show the number of subgroups of order p is the same as the number of subgroups of index p. But this boils down to showing that the number of 1-dimensional $\mathbf{F}_p$-vector spaces in $(\mathbf{F}_p)^n$ is equal to the number of 1-codimensional (i.e., $n-1$-dimensional) $\mathbf{F}_p$-vector spaces in $(\mathbf{F}_p)^n$. Observe both numbers are given by the gaussian binomial coefficient [2, pp. 3–5], which is a center symmetric quantity:

$$\binom{n}{n-1}_p = \binom{n}{1}_p = \frac{1-p^n}{1-p},$$

as desired. □

8.2. **[1, No. 5.2.14].** For any group G define the *dual group* $\hat{G}$ of G to be the set of all homomorphisms from G into the multiplicative group of roots of unity in $\mathbf{C}$. Define a group operation in $\hat{G}$ by pointwise multiplication of functions: if χ and ψ are homomorphisms from G into the group of roots of unity, then $\chi\psi$ is the homomorphism given by $(\chi\psi)(g) = \chi(g)\psi(g)$ for all $g \in G$.

(a) This operation on $\hat{G}$ makes $\hat{G}$ into an abelian group.

Proof. To verify that $\hat{G}$ is abelian.

- $\hat{G}$ is a set closed under the binary operation given by pointwise multiplication.
- Associativity and commutativity of elements in $\hat{G}$ follows from the same properties of elements in $\mathbf{C}$.
- The homomorphism $\mathbf{1}_G \in \hat{G}$ that sends $g \in G$ to $1 \in \mathbf{C}$ is the identity.
  - One may check that for all $\chi \in \hat{G}$ and all $g \in G$,
$$\mathbf{1}_G\chi(g) = \chi(g) = \chi\mathbf{1}_G(g).$$
- For each $\chi \in \hat{G}$, the map $\chi^{-1} \in \hat{G}$ given by $g \mapsto (\chi(g))^{-1}$ is the (left and right) inverse to χ.
  - One may check that for all $g \in G$,
$$\chi\chi^{-1}(g) = \mathbf{1}_G(g) = \chi^{-1}\chi(g).$$

As desired, $\hat{G}$ is seen to be an abelian group. □

(b) If G is a finite abelian group, then $\hat{G} \cong G$.

Proof. G is a finite abelian group, whence by the fundamental theorem of finitely generated abelian groups

$$G = \prod_{j=1}^{r} \langle x_j \rangle.$$

Suppose $n_i = |x_i|$ and define for each i,

$$\chi_i \in \hat{G} \quad \text{such that} \quad \chi_i\colon \prod_{j=1}^{i-1} 1 \times x_j \times \prod_{j=i+1}^{r} 1 \mapsto e^{2\pi i/n_i}$$

and that

$$\prod_{j=1}^{k-1} 1 \times x_k \times \prod_{j=k+1}^{r} 1 \mapsto e^0 = 1 \quad \text{for } k \neq i.$$

We've defined χ_i on generators of G, so on each element of G. Now we want to show χ_i has order n_i. Let $g \in G$ and $b \in \mathbf{N}$. Consider

$$\chi_i^b(g) = (\chi_i(g))^b = e^{2\pi i b/n_i} = 1,$$

occurring if and only if b is a multiple of n_i. So $|\chi_i| = \min\{b \in \mathbf{N} : b = kn_i\} = n_i$. We now identify each x_i with $\prod 1 \times x_i \prod 1$, the coordinate axis generators.

Observe if $\psi \in \hat{G}$, then we can write ψ uniquely as the product of the χ_i. That is, we consider the image under ψ of each coordinate generator x_i: $\psi(x_i) = e^{2\pi i/c_i/n_i}$ for some $c_i \in \{0, \ldots, n_i - 1\}$ (if ψ did not map x_i to such a multiple of $e^{2\pi i/n_i}$, we'd obtain the contradiction $1 \neq (\psi(x_i))^{n_i} = \psi(1) = 1$.

If follows that $\psi = \chi_1^{c_1}\chi_2^{c_2} \cdots \chi_r^{c_r}$. By the recognition theorem for direct products, (maybe abusing notation)

$$\bigcap_{j=1}^{r} \langle \chi_j \rangle = \{1_G\}$$

and $\langle \chi_j \rangle \lhd \hat{G}$, so

$$\hat{G} = \langle \chi_1 \rangle \times \cdots \times \langle \chi_r \rangle.$$

Now each coordinate axis subgroup of the same index i in G and $\hat{G}$ are isomorphic to C_{n_i}, so $G \cong \hat{G}$. See also [3]. □

8.3. **[1, No. 6.1.7].** Subgroups and quotient groups of nilpotent groups are[2] nilpotent.

Proof. We proceed by lower central series. Let G be nilpotent of class c. Then $\gamma_c(G) = \{1\}$. If $H \leqslant G$, then $\gamma_c(H)$ is also trivial. Well, observe that $\gamma_0(H) \leqslant \gamma_0(G)$ and for all $n \geqslant 1$ we have

$$\gamma_n(H) = [H, \gamma_{n-1}(H)] \leqslant [G, \gamma_{n-1}(G)] = \gamma_n(G).$$

So if $\gamma_c(G) = \{1\}$, then $\gamma_c(H) = \{1\}$. Therefore H is nilpotent, of class at most c.

For the quotient, let $N \lhd G$ and consider the canonical projection $\pi\colon G \to G/N$. For all $gN \in \gamma_n(G/N)$ there's a $g \in \gamma_n(G)$ such that $g \mapsto_\pi gN$. So the map from $\gamma_n(G)/N$ to $\gamma_n(G/N)$ is onto for all n. Whence G/N is nilpotent whenever G is. See also [4]. □

We exhibit a group G which possesses a normal subgroup H such that both H and G/H are nilpotent but G is not nilpotent.

Demo. Try S_3. Clearly $S_3/A_3 \cong \mathbf{Z}/2\mathbf{Z}$ and $A_3 \cong \mathbf{Z}/3\mathbf{Z}$ are nilpotent. Yet $[S_3, S_3] = A_3$ and $[S_3, A_3] = A_3$, so the lower central series stabilizes away from $\{1\}$.

8.4. **[1, No. 6.1.10].** D_{2n} is nilpotent if and only if n is a power of 2.

Proof. We know $D_{2n} \cong C_2 \rtimes_\varphi C_n$, the semidirect product with the appropriate twist defined $\varphi(s)(r) = r^{-1}$.

For contradiction, suppose *both* (i) $n \neq 2^a$ for any $a \in \mathbf{Z}_{\geqslant 0}$ and (ii) D_2n is nilpotent. Now if $s, r \in D_{2n}$ with $|s| = 2$, $|r| = n$, then $(|s|, |r|) = 1$. But then [DF04, page 192] $rs = sr$, a contradiction. ("A finite group G is nilpotent if and only if whenever $a, b \in G$ with $(|a|, |b|) = 1$, then $ab = ba$.") So D_{2n} isn't nilpotent.

On the other hand, if $n = 2^a$ for some nonnegative integer a, then D_{2n} is the direct product of its Sylow subgroups (D_{2n} is a 2-group!), hence nilpotent. □

8.5. **[1, No. 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 $\bar{G} = G/N$.

(a) With Frattini's argument, $N_{\bar{G}}\left(\bar{P}\right) = \overline{N_G\left(P\right)}$.
(b) From above, $N_{\bar{G}}\left(\bar{P}\right) = \overline{N_G\left(P\right)}$.

TODO

[2] Even in the infinite case.

8.6. **[1, No. 6.1.24]. Definition.** 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 $\Phi(G) = G$).

Say an element x of G is a *nongenerator* if for every proper subgroup H of G, $\langle x, H\rangle$ is also a proper subgroup of G. If $|G| > 1$, then $\Phi(G)$ is the set of nongenerators of G.

Given. A nontrivial group G, the set $\mathscr{M}$ of maximal subgroups of G, maximal subsets M in $\mathscr{M}$.

To prove. The intersection of all $M \in \mathscr{M}$ is $\Phi(G)$.

Proof. ($\subset$) Suppose

$$x \in \bigcap_{M \in \mathscr{M}} M.$$

Then for any $H \lneq G$, there's a maximal $M_H \in \mathscr{M}$ such that $H \leqslant M$. Since $x \in M_H$, we have $\langle x, H\rangle \leqslant M_H \lneq G$. So x is a *nongenerator*. Thus $x \in \Phi(G)$.

($\supset$) Let $x \in \Phi(G)$. We'll show that x is in every maximal subgroup $M \in \mathscr{M}$. Since each M is proper, if $x \notin M$, then $\langle x, M\rangle = G$, a contradiction. So $x \in M$. □

8.7. **[1, No. 6.1.25].** With G be a finite group, $\Phi(G)$ is nilpotent.[3]

Given. A finite group G, its Frattini subgroup $\Phi(G)$.

To prove. For each prime p, for each $P \in \mathrm{Syl}_p(\Phi(G))$, we have $P \trianglelefteq \Phi(G)$. By the recognition theorem, $\Phi(G)$ will be the product of its Sylow subgroups. We'll conclude that $\Phi(G)$ nilpotent.

Proof. Observe that $\Phi(G)$ is characteristic in G. (Why? If $\sigma \in \mathrm{Aut}(G)$, then σ permutes maximal subgroups. Thus σ fixes their intersection $\Phi(G)$.) The hypotheses of the Frattini argument are met—$\Phi(G) \trianglelefteq G$, G is a finite group, $P \in \mathrm{Syl}_p(\Phi(G))$—so

$$G = \Phi(G)N_G(P).$$

It follows[4] that

$$\Phi(G) = G \cap \Phi(G) = \Phi(G)N_G(P) = N_{\Phi(G)}(P).$$

So $P \trianglelefteq \Phi(G)$.

We see every Sylow subgroup of $\Phi(G)$ is normal. With a familiar argument from Lagrange, the intersection of any distinct two Sylow subgroups is trivial. By the recognition theorem for direct products

$$\Phi(G) = \prod_{i=q}^{r} P_i \quad \text{where} \quad |\Phi(G)| = \prod_{i=1}^{r} p_i^{a_i} \quad \text{is the prime factor decomposition with } P_i \in \mathrm{Syl}_{p_i}(\Phi(G)).$$

Since $\Phi(G)$ is the direct product of its Sylow subgroups, $\Phi(G)$ is nilpotent. □

8.8. **[1, No. 6.1.26].** Suppose p is a prime, P is a finite p-group and define $\bar{P} = P/\Phi(P)$.

(a) $\bar{P}$ is an elementary abelian p-group.

Proof. We start by finding the order of elements in $\bar{P}$. Let $\bar{x} \in \bar{P}$. Then $\bar{x}^p = x^p\Phi(P)$. We'll now show $x^p \in M$ for all maximal M.

By way of contradiction (similar to [1, No. 5.2.8]) suppose that $x^p \notin M$. We're forced to accept $x \notin M$. Now $|P/M| = p$, a prime. Then the quotient P/M is cyclic and of the form $\langle x\rangle M$. But

$$1 \cdot M = (xM)^p = x^p M, \text{ so } x^p \in M, \text{ a contradiction.}$$

So $x^p \in M$.

[3]Hint: Use Frattini's Argument to prove that every Sylow subgroup of $\Phi(G)$ is normal in G.
[4]I've seen other directions for this proof, so this line of reasoning may not pan out.

It follows that $x^p \in \Phi(P)$. So every nonidentity element $\bar{x} \in \bar{P}$ has order p.

Now we'll verify the commutativity of $\bar{P}$. Since for each maximal $M \in \mathscr{M}$ the quotient P/M is cyclic, we must have the commutator embedded: $P^{(1)} \leqslant M$. So

$$P^{(1)} \leqslant \bigcap_{M \in \mathscr{M}} M = \Phi(P).$$

We conclude that $\bar{P}$ is elementary abelian.

(b) If N is any normal subgroup of P such that P/N is elementary abelian, then $\Phi(P) \leqslant N$.

To prove. The Frattini subgroup $\Phi(P)$ is the smallest normal subgroup (of a p-group P) such that the quotient of P by $\Phi(P)$ is elementary abelian. That is, if $\varphi\colon P \to A$ is any group homomorphism of P into elementary abelian A, then φ factors (uniquely!) through $P/\Phi(P)$ and the following diagram commutes.

Proof. Supposing N is a normal subgroup of P such that P/N is elementary abelian, we have

$$\prod_{i=1}^{r} \langle x_i N \rangle.$$

Which subgroups of P/N are maximal? Those generated by $r-1$ of the $x_i N$, call them $M_i/N = \langle x_j N : j \neq i \rangle$. Being subgroups of a direct product each with one coordinate trivial,

$$\bigcap_{\forall i} M_i/N = \{1 \cdot N\}.$$

Then pulling back, $\cap M_i = N$. Note each subgroup M_i is maximal in P. Whence

$$\Phi(P) \leqslant \bigcap_{\forall i} M_i = N,$$

as desired. Since normal subgroups correspond to homomorphisms out of P, the conclusion follows. □

$$\begin{tikzcd} P \arrow[r, "\pi"] \arrow[dr, "\varphi"'] & P/\Phi(P) \arrow[d, dashed, "\exists!"] \\ & A \end{tikzcd}$$

(c) Let $\bar{P}$ be elementary abelian of order p^r. From [1, No. 6.1.24], it follows that:

If $\bar{x}_1, \ldots, \bar{x}_r$ are any basis for the r-dimensional vector space $\bar{P}$ over $\mathbf{F}_p$ and if x_i is any element of the coset $\bar{x}_i$, then $P = \langle x_1, \ldots, x_r \rangle$.

- That is suppose $\bar{P} \cong (\mathbf{F}_p)^r$ with a basis $\{\bar{x}_i : i = 1, \ldots, r\}$. Suppose $x_i \in \bar{x}_i$ for each i. By way of contradiction, suppose $P \neq \langle x_i : i = 1, \ldots, r \rangle$. Then, with out loss of generality, there's a $x_{r+1} \in P \setminus \langle x_i : \forall i \neq r+1 \rangle$ with $x_{r+1} \notin \Phi(P)$. Passing to the quotient, $\langle \bar{x}_{r+1} \rangle \cap \underbrace{\langle \bar{x}_i : \forall i \neq r+1 \rangle}_{\text{a basis?}} = \{1\}$.

  Contradiction.
- So $P = \langle x_i : i = 1, \ldots, r \rangle$ as desired.

Conversely,[5] if $y_1, \ldots, y_s$ is any set of generators for P, then $s \geqslant r$.

- Let $P = \langle y_1, \ldots, y_s \rangle$. Again for contradiction, suppose $s < r$. Then there's basis of $\bar{P}$ that contains some $\bar{y}_r$ such that $\langle \bar{y}_r \rangle \cap \langle \bar{y}_i : i = 1, \ldots, s \rangle = \{\bar{1}\}$. Choose $y_r \in \bar{y}_r$. Now $y_r \in P$ and $\underbrace{y_r \notin \Phi(P)}_{\bar{y}_r \neq \bar{1}}$, but $P = \langle y_1, \ldots, y_s \rangle = \langle y_1, \ldots, y_s, y_r \rangle$. Therefore $y_r \Phi(P)$, a contradiction. Thus $s \geqslant r$.

Now *Burnside's Basis Theorem* follows: a set $y_1, \ldots, y_s$ is a minimal generators set for P if and only if $\bar{y}_1, \ldots, \bar{y}_s$ is a basis of $\bar{P}$.

- In the setup above, if $r < s$, then set of generators for P is not minimal.
- If $r = s$, the set of generators for P *is minimal.*
- If $r > s$, then the set $\bar{y}_1, \ldots, \bar{y}_s$ is not a basis.

Any minimal generating set for P has r elements.

- From argument above, a generating set of s elements for P is minimal if $s = r$ given $\bar{P} \cong (\mathbf{F}_p)^r$.

(d) If $\bar{P}$ is cyclic, then P is too. It follows that if P/P' is cyclic, then so is P.

Proof. If $\bar{P}$ is cyclic, then $P\langle x \rangle$. Conversely, if P is cyclic, then $\Phi(P)$ is trivial and $\bar{P} \cong P$ is cyclic too. Moreover, if P/P' is cyclic, then $\bar{P}$ is cyclic, because there's a natural surjection $\pi : P/P' \to \bar{P}$. Namely the quotient maps

$$P \to P/P' \xrightarrow{\pi} \bar{P} \quad \text{such that, in the subgroups,} \quad \Phi(P) \to \Phi(P)/P' \xrightarrow{\pi} \{\bar{1}\}.$$

(e) Let σ be any automorphism of P of prime order q with $q \neq p$. If σ fixes the coset $x\Phi(P)$ then σ fixes some element of this coset.[6]

Given. $\sigma \in \text{Aut}(P)$ such that $q = |\sigma|$, $p \neq q$, and q prime.

To prove. If $\sigma(\bar{x}) = \bar{x}$ then there's $x \in \bar{x}$ such that $\sigma(x) = x$.

Proof. That $\Phi(P)$ char P implies σ induces $\bar{\sigma} \in \text{Aut}\left(\bar{P}\right)$ is clear. Now for the fixed point. We do assume that $\sigma(\bar{x}) = \bar{x}$. With $|\sigma| = q$, either for all $x \in \bar{x}$, $\sigma(x) = x$ (and we're done) or $\sigma^q(x) = x$. Now σ restricted to $\bar{x}$ has cycle type consisting of q's and 1's. Moreover, σ permutes the p^a elements of $\bar{x}$. Since $q \nmid p^a$, it's true that $p^a = qd + r$ by the Euclidean algorithm with $r \neq 0$. But this nonzero remainder is the number of points in $\bar{x}$ fixed by σ. Thus σ fixes at least $r > 0$ elements of $\bar{x}$. □

(f) (Hall-Burnside) With parts (c) and (e), every nontrivial automorphism of P of order prime to p induces prime a nontrivial automorphism on $P/\Phi(P)$. Any group of automorphisms of P which has order prime to p is isomorphic to a subgroup of $\text{Aut}\left(\bar{P}\right) = \text{GL}_r(\mathbf{F}_p)$.

Given. $\sigma \in \text{Aut}(P)$ is a nontrivial automorphism with $(|\sigma|, p) = 1$.

To prove. σ is a nontrivial automorphism of $\bar{P}$.

Proof. For contradiction, suppose σ is trivial on $\bar{P}$. Then as in (e), we see σ fixes at least one element in each coset $\bar{x} \in \bar{P}$. Now choose $x_i \in \bar{x}_i$ such that σ fixes x_i. By Burnside's basis theorem (c) we know $P = \langle x_i : \forall i \in \{1, \ldots, r\} \rangle$ (recall $r = \left|\bar{P}\right|$). But then $\sigma = \text{id}_P$, a contradiction. So σ induces a nontrivial automorphism of $\bar{P} \cong (\mathbf{F}_p)^r$.

---

[5] We assume that every minimal generating set for an r-dimensional vector space has r elements, i.e., every minimal basis has r elements.

[6] Hint 1: Note that since $\Phi(P)$ is characteristic in P, every automorphism of P induces an automorphism of $P/\Phi(P)$. Hint 2: Use the observation that σ acts as a permutation of order 1 or q on the p^a elements in the coset $x\Phi(P)$.

Now, if $A \subset \mathrm{Aut}(P)$ and $(|A|, p) = 1$, then for $\sigma, \tau \in A$, nontrivial and distinct, both σ and τ induce nontrivial automorphisms of $\bar{P}$. (If σ and τ are the same automorphism of $\bar{P}$, then by argument above $\mathrm{id}_P = \sigma^{-1} \circ \tau$, and so $\sigma = \tau$.)

So there's a monomorphism f from A into $\mathrm{Aut}(P)$ (taking σ to its unique induced $\bar{\sigma}$). By the first isomorphism theorem,

$$A \cong f(A) \leqslant \mathrm{Aut}(\bar{P}) \cong \mathrm{GL}_r(\mathbf{F}_p),$$

as desired. □

8.9. **[1, No. 6.1.31].** For any group G a *minimal normal subgroup* is a normal subgroup M of G such that the only normal subgroups of G which are contained in M are 1 and M. We'll show[7] every minimal normal subgroup of a finite solvable group is an elementary abelian p-group for some prime p.

Given. A finite solvable group G and a minimal normal subgroup $M \lhd G$.

To prove. M is an elementary abelian p-group, by arguing the commutator subgroup M' is trivial and finding a p for which the image of M under the pth power map M^p is also trivial.

Proof. Since M' and M^p are characteristic subgroups of M, it suffices only to prove that $M \neq M'$ and, for a prime p, $M \neq M^p$.

$$\begin{tikzcd}[column sep=small]
& G \arrow[dl, dash] \arrow[dr, equal] & \\
M \arrow[dr, equal] & & G' \arrow[dl, dash] \\
& M' = \underbrace{M \cap G'}_{\text{verify}} &
\end{tikzcd}$$

By the diamond isomorphism theorem,

$$G/G' \cong M/M',$$

which, given the hypothesis that G is solvable, implies

$$\{1 \cdot G'\} \lneq G/G', \quad \text{i.e.,} \quad \{1 \cdot M'\} \lneq M/M'.$$

We see M' is a proper normal subgroup of M. By the minimal normal hypothesis, M' must be trivial. It follows that M is abelian.

Now to find p such that M^p is also trivial. Take the smallest prime p dividing the order $|M|$. By Cauchy's theorem, there's a cyclic group $\langle x \rangle$ of order p in M. But then there's $x' \in \langle x \rangle$ such that $x' \in M \setminus M^p$. We see

$$M \neq M^p \quad \text{thus} \quad M^p = \{1\}.$$

We conclude M is elementary abelian. □

8.10. **Classifying simple groups (without Feit–Thompson!)** Suppose G is a group and $60 < |G| \leqslant 100$. If G is simple, then G is abelian.

Proof. Consider G a group of order $n \in \{61, \dots, 100\}$. We'll cast out from consideration all groups that are either abelian, or that contain nontrivial proper normal subgroups.

- We won't consider any p-group P as
  - either P is cyclic (thus abelian) or

[7]Hint: If M is a minimal normal subgroup of G, consider its characteristic subgroups: M' and $\langle x^p : x \in M \rangle$.

- P is nilpotent (thus solvable, thus not simple).

- We won't consider any group H of order pq, p^2q, or pqr, for primes p, q, r, as
  - by Sylow's theorem, each such H has a nontrivial proper normal subgroup.
- We won't consider any group J of order $p^a q^b$, for p, q primes, as
  - we'll then have reason to prove Burnside's lemma in [DF04, chapter 12],
  - thus showing all groups of order $p^a q^b$ are solvable (thus not simple).

What remains?

- $|G| = 84 = 2^2 \cdot 3 \cdot 7$.
  - By Sylow's theorem, $n_7 = 1$, so $H_7 \lhd G$, thus G is not simple.
- $|G| = 90 = 2 \cdot 3^2 \cdot 5$.
  - Now $n_5 \in \{1, 6\}$, $n_3 \in \{1, 10\}$, and $n_2 \in \{1, 3, 5, 9, 15, 45\}$.
  - Suppose each $n_i > 1$ or we're done.
  - Counting nontrivial elements, we're forced to accept the 3-subgroups of the form $(\mathbf{Z}/3\mathbf{Z})^2$.
  - By above, we're also forced to accept 45 Sylow 2-subgroups, as
$$90 = |G| = \underbrace{1}_{\text{order } 1} + \underbrace{45}_{2} + \underbrace{20}_{3} + \underbrace{24}_{6}.$$
  - So consider G acting by conjugation on the coset space G/H_5.
    * We've the permutation representation $\varphi \colon G \to S_6$.
    * Suppose ker $\varphi = N$.
    * What's N?
      · $N \leqslant N_G(H_5)$.
      · $N \neq G$ as then $H_5 \lhd G$, a contradiction.
      · So N must be $\{1\}$.
    * Then "$G \leqslant S_6$" by identification of G with its image.
      · Wherefore $G \leqslant A_6$ since G has no subgroup of index 2
      · But A_6 cannot have a subgroup of index 4 as $360 \nmid 4!$,
      · i.e., there's only a trivial action of A_6 on the coset space A_6/G
      · which gives *another contradiction.*
    * Therefore $N \neq \{1\}$.
      · So $\{1\} <$ ker $\varphi \lhd G$.
  - So if $|G| = 90$, then G has a normal subgroup.

Given the hypotheses, we've demonstrated that if G is simple, then G is abelian. □

References

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

[2] A. Prasad, "Counting subspaces of a finite vector space," *Resonance*, vol. 15. pp. 977–987, 31-Nov-2010 [Online]. Available: http://arxiv.org/abs/1006.2193

[3] K. Conrad, "Characters of finite abelian groups," Oct. 2018 [Online]. Available: http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/charthy.pdf

[4] B. Conrad, "Solvable and Nilpotent Groups," Dec. 2016 [Online]. Available: https://math.stanford.edu/~conrad/210BPage/handouts/SOLVandNILgroups.pdf