

Contents

Chapter 1	1
1A	1
1B	4
1C	6
1D	8
1E	12
1F	14
1G	15
Chapter 2	16
2A	16
2B	19
2C	21
2D	22
Chapter 3	22
3A	22
3B	26
3C	30
3D	34
3E	35
3F	37
Chapter 4	38
4A	39
4B	44
4C	45
4D	46
Chapter 5	49
5A	49
5B	52
5C	53
5D	56
5E	58

Contents

Chapter 6	59
6A	59
6B	63
6C	66
Chapter 7	67
7A	68
7B	71
7C	71
7D	72
Chapter 8	72
8A	72
8B	77
8C	81
8D	83
Chapter 9	85
9A	85
9B	87
9C	89
9D	91
Chapter 10	93
10A	93
10B	96
10C	96

Solutions

Solutions to problems in Isaacs's *Finite Group Theory* book.

1A

[1A.1] Let G act on the p cosets of H . This gives a homomorphism $G \rightarrow S_p$; if $K \leq H$ is the kernel of this homomorphism, then $[G : K]$ divides $p!$. Since no prime smaller than p divides $|G|$ and no prime larger than p divides $p!$, it must be that $[G : K] = p = [G : H]$, so that $K = H$ is normal in G .

[1A.2] Let K act on the right cosets of H . Then for $g \in G$, let $\mathcal{O}$ be the orbit containing the coset Hg . Note that $Hgk = Hg$ if and only if $k \in H^g$, so that the stabilizer of Hg in K is $K \cap H^g$. So we see the orbit $\mathcal{O}$ has size $[K : K \cap H^g]$. Since these cosets are disjoint, and each has size $|H|$, we see then that

$$|HgK| = \left| \bigcup_{X \in \mathcal{O}} X \right| = |H| \cdot |\mathcal{O}| = |H| \cdot [K : K \cap H^g] = \frac{|H| \cdot |K|}{|K \cap H^g|}$$

[1A.3]

(a) We have from the previous problem

$$\frac{|H| \cdot |K|}{|K \cap H|} = |HK| \leq |G|$$

since $HK \subset G$. Dividing both sides by $|K|$ gives $[H : H \cap K] \leq [G : K]$. Equality happens precisely when $|HK| = |G|$, and so $HK = G$, from the above.

(b) We have

$$[G : H][H : H \cap K] = [G : H \cap K] = [G : K][K : H \cap K]$$

Since $[G : H]$ and $[G : K]$ are relatively prime, we have $[G : K]$ dividing $[H : H \cap K]$. By part (a), we have $[H : H \cap K] \leq [G : K]$, and hence these indices must be equal. Again by part (a), this implies $HK = G$.

[1A.4] Suppose $G = HK$, and let $x, g \in G$. Note we can write $x = hk$ for $h \in H$ and $k \in K$. Also we can write $kg = ab$ for $a \in H$ and $b \in K$. Then we have

$$g = k^{-1}a(kk^{-1}b) = k^{-1}h^{-1}(hah^{-1})hk(k^{-1}b) \in H^xK$$

Since g was arbitrary, we see $G = H^xK$. Doing something similar for $y \in G$ shows also that $G = H^xK^y$. Of course this means that if $G = HH^x$, then $G = HH = H$.

[1A.5] First assume G acts transitively on $\Omega \times \Lambda$ and fix $\alpha \in \Omega$ and $\beta \in \Lambda$. If $g \in G$, suppose $(\alpha, \delta)^g = (\lambda, \beta)$, for example by choosing $\delta = \beta \cdot g^{-1}$. Now choose $h \in G$ such that $(\lambda, \beta)^h = (\alpha, \beta)$. Then $h \in G_\beta$ and $gh \in G_\alpha$. Since g was arbitrary, we have shown that $G = G_\alpha G_\beta$.

Conversely, suppose $G = G_\alpha G_\beta$. To show G is transitive on $\Omega \times \Lambda$, it is enough to show for any pair (γ, δ) , there is a $g \in G$ with $(\alpha, \beta)^g = (\gamma, \delta)$. Since G is transitive on Ω , choose $g \in G$ with $\alpha \cdot g = \gamma$, and let $\beta \cdot g = \epsilon$. Since G is transitive on Λ , choose $h \in G$ with $\epsilon \cdot h = \delta$. From the previous problem, $G = G_\alpha^x G_\beta^y$ for any $x, y \in G$. In particular, if $\alpha \cdot x = \gamma$ and $\beta \cdot y = \delta$, then

$$G = G_\alpha^x G_\beta^y = G_\gamma G_\delta$$

So we can write $h = ab$ with $a \in G_\gamma$ and $b \in G_\delta$. Since $\epsilon \cdot h = \delta$, and b fixes δ , we must have $\epsilon \cdot a = \delta \cdot b^{-1} = \delta$. But then

$$(\alpha, \beta)^{ga} = (\gamma, \epsilon)^a = (\gamma, \delta)$$

with the last equality relying on $a \in G_\gamma$. Thus G is indeed transitive in its product action.

[1A.6] Note that from the orbit-stabilizer theorem, if $\mathcal{O}_\alpha$ is the orbit of G containing $\alpha \in \Omega$, then $[G : G_\alpha] = |\mathcal{O}_\alpha|$. We can rewrite this as $|G_\alpha| = |G|/|\mathcal{O}_\alpha|$. Noting that $\chi(g)$ just counts how many point stabilizers g is in, we then have

$$\sum_{g \in G} \chi(g) = \sum_{\alpha \in \Omega} \sum_{g \in G_\alpha} 1 = \sum_{\alpha \in \Omega} |G_\alpha| = \sum_{\alpha \in \Omega} \frac{|G|}{|\mathcal{O}_\alpha|}$$

Now Ω can be partitioned into finitely many orbits $\mathcal{O}_1, \dots, \mathcal{O}_n$. So the above sum equals

$$\sum_{\alpha \in \Omega} \frac{|G|}{|\mathcal{O}_\alpha|} = \sum_{i=1}^n \sum_{\alpha \in \mathcal{O}_i} \frac{|G|}{|\mathcal{O}_i|} = \sum_{i=1}^n |G| = n|G|$$

[1A.7] Let χ be the permutation character of G on the right cosets of $H < G$. This is a transitive action, so by the previous problem $\sum \chi(g) = |G|$. Meanwhile, if we restrict the action to H on its own right cosets, there are at least 2 orbits: the single point $\{H\}$ (since H is a subgroup), and the other orbits. Hence, again by the previous problem, $\sum \chi(h) \geq 2|H|$. Write $G \setminus H = R \sqcup S$, where $R = \{g \in G \setminus H \mid \chi(g) = 0\}$. Then we see

$$|G| = \sum_{g \in H} \chi(g) + \sum_{g \in R} \chi(g) + \sum_{g \in S} \chi(g) \geq 2|H| + |S|$$

So $|S| \leq |G| - 2|H|$. Since $|S| + |R| = |G| - |H|$, this means $|R| \geq |H|$. But R is exactly those elements of G that don't lie in any point stabilizer, and hence do not lie in any conjugate of H .

[1A.8]

(a) This is clearly an action on the set of all n -tuples, since:

$$\begin{aligned} (x_1, \dots, x_n) \cdot 0 &= (x_1, \dots, x_n) \\ (x_1, \dots, x_n) \cdot k \cdot m &= (x_{1+k}, \dots, x_{n+k}) \cdot m \\ &= (x_{1+k+m}, \dots, x_{n+k+m}) \\ &= (x_1, \dots, x_n) \cdot (k+m) \end{aligned}$$

To see this action leaves Ω invariant, note that from $x_1 \cdots x_n = 1$ we have that

$$x_{1+k} \cdots x_{n+k} = (x_1 \cdots x_k)^{-1} (x_1 \cdots x_n) (x_1 \cdots x_k) = (x_1 \cdots x_k)^{-1} (1) (x_1 \cdots x_k) = 1$$

(b) Since C is cyclic of order p , it only has 2 subgroups: the trivial ones. So a point stabilizer in C is either the trivial subgroup, or all of C . Let Ω_0 be the orbits of size 1 (the fixed points), and $\mathcal{O}$ the orbits of size p . Then we have

$$|\Omega| = |\Omega_0| + p|\mathcal{O}|$$

However, $|\Omega| = |G|^{p-1}$, since we can pick $x_2, \dots, x_p$ arbitrarily, and there is exactly one x_1 that makes the product $x_1 \cdots x_p = 1$. Since p divides $|G|$ by hypothesis, we see from the above equation that $|\Omega_0| \equiv 0 \pmod{p}$.

Now $(x_1, \dots, x_n) \in \Omega_0$ precisely when $x_1 = x_2 = \cdots = x_n$. Letting $x \in G$ be this common value, we see then that $x^p = 1$. Meanwhile, if we have an $x \in G$ with $x^p = 1$, then $(x, \dots, x) \in \Omega_0$. So $|\Omega_0|$ counts the elements of order dividing p in G . There is only one element in G of order 1, so the number of elements of order p is

$$|\Omega_0| - 1 \equiv -1 \pmod{p}$$

[1A.9]

From the previous problem, we know G has an element $x \in G$ of order p , so that $H = \langle x \rangle \leq G$ is a subgroup of order p . Suppose $K \leq G$ is another subgroup of order p . Since $HK \subset G$ and $H \cap K = \{1\}$ (because p is prime), then from [1A.2] we see

$$pm = |G| \geq |HK| = \frac{|H| \cdot |K|}{|H \cap K|} = |H| \cdot |K| = p^2$$

And this contradicts $m < p$. Thus K does not exist, and H is the unique subgroup of order p .

[1A.10]

- (a) Let Hx be a right coset of H . Then for $h \in H$, we have $Hxh = Hx$ if and only if $xhx^{-1} \in H$. If this is true for all $h \in H$, then this is equivalent to $H^x = H$, so that $x \in N_G(H)$. Thus the cosets of H in G that are invariant under H are precisely those cosets of H in $N_G(H)$, of which there are $[N_G(H) : H]$.
- (b) Let H act on its right cosets in G . By Lagrange's theorem and the orbit-stabilizer theorem, all non-trivial orbits of H have size divisible by p . If $\mathcal{O}_0$ are the size 1 orbits, then

$$[G : H] \equiv |\mathcal{O}_0| \pmod{p}$$

By hypothesis $[G : H]$ is divisible by p , and hence so is $|\mathcal{O}_0|$, which is equal to $[N_G(H) : H]$ by part (a).

1B

[1B.1]

- (a) If $P \leq S$ then of course $PS = S$ is a subgroup. Conversely, if PS is a subgroup, then let $|S| = p^a$, $|P| = p^b$, and $|P \cap S| = p^c$. From [1A.2], we see that

$$|PS| = \frac{|P| \cdot |S|}{|P \cap S|} = p^{a+b-c}$$

Since $|PS|$ divides $|G|$, and $S \leq G$ is a Sylow subgroup, it must be that $a + b - c \leq a$, which is to say that $c \geq b$. Since $c \leq b$ because $P \cap S \leq P$, we see $b = c$ and thus $P \cap S = P$ as desired.

- (b) Let $S \triangleleft G$ be a normal Sylow subgroup, and let $P \leq G$ be another Sylow subgroup. From the previous part, since PS is a subgroup, we have $P \leq S$ and, since $|P| = |S|$, it must be that $P = S$. Thus S is the only Sylow subgroup of G , and thus $\mathbf{O}_p(G) = S$ is characteristic in G .

[1B.2]

Let $P \triangleleft G$ be a normal p -subgroup of G . If $S \leq G$ is a Sylow subgroup of G , then PS is a subgroup of G , so from the previous problem $P \leq S$. Since this is true for all Sylow p -subgroups, P is contained in their intersection: $P \leq \mathbf{O}_p(G)$.

[1B.3]

$S \triangleleft N$ by definition, so from part (b) of [1B.1] we have that S is characteristic in N . Since $N \triangleleft N_G(N)$, Lemma 1.10 shows $S \triangleleft N_G(N)$, so that $N_G(N) \leq N_G(S) = N$. Of course this means $N = N_G(N)$.

[1B.4]

Let p^n be the largest power of p dividing $|G|$, with $n > 0$. By Cauchy's theorem, there is a subgroup $P_1 \leq G$ of order p . If $n = 1$, P_1 is a Sylow p -subgroup of G and we're done. Otherwise, $[G : P_1]$ is divisible by p , so [1A.10] shows $[N_G(P_1) : P_1]$ is divisible by p . There is thus a subgroup of order p in $N_G(P_1)/P_1$, again by Cauchy's theorem, and that subgroup corresponds to a subgroup $P_2 \geq P_1$ of G , with $[P_2 : P_1] = p$ so that $|P_2| = p^2$. Again, if

$n = 2$, we're done. Otherwise we continue this way, constructing $P_3, \dots, P_n$ with P_n a Sylow p -subgroup of G .

[1B.5]

- (a) $\theta(H)$ has order dividing $|H|$, as an image of H , so $\theta(H)$ is a π -group. If $L \triangleleft G$ is the kernel of θ , then $[K : \theta(H)] = [G : HL]$ is a divisor of $[G : H]$, and hence no prime in π divides it. Thus $\theta(H) \leq K$ is a Hall π -subgroup.
- (b) Let $P \leq K$ be a Sylow p -subgroup, and let $S = \theta^{-1}(P)$. Then $[G : S]$ is not divisible by p . If $H \leq S$ is a Sylow p -subgroup of S , then it is also one of G . From part (a), $\theta(H)$ is a Sylow p -subgroup of K , and since $\theta(H) \leq \theta(S) = P$, we see $\theta(H) = P$.
- (c) From part (b) every Sylow p -subgroup of K has a Sylow p -subgroup of G that maps to it, and hence by part (a) θ induces a surjective map $\text{Syl}_p(G) \rightarrow \text{Syl}_p(K)$, from which the cardinality inequality follows.

[1B.6]

From [1A.2] we see that $[K : H \cap K] = [HK : H]$. Since this latter index divides $[G : H]$, it is not divisible by any prime in π . Since $H \cap K \leq H$, we see it is a π -group, and hence $H \cap K \leq K$ is a Hall π -subgroup.

[1B.7]

- (a) Let $K, L \triangleleft G$ be normal π -subgroups. Then by [1A.2] $|KL|$ is a π -number, so $KL \triangleleft G$ is also a normal π -subgroup. Hence if N is the product of all normal π -subgroups of G , it is (by induction) a normal π -subgroup, and must be the unique largest one, containing all the others.
- (b) Let $H \leq G$ be a Hall π -subgroup. Since HN is a subgroup of G , the previous problem shows $H \cap N$ is a Hall π -subgroup of N . But N is a π -group, so that $H \cap N = N$, and hence $N \leq H$. Because H was arbitrary, we see N is contained in all Hall π -subgroups of G .
- (c) If $g \in G$, and $H \leq G$ is a Hall π -subgroup, then H^g is a Hall π -subgroup of G . That is, conjugation by g is a permutation on the Hall π -subgroups of G . Thus if N is their intersection, we have

$$N^g = \left(\bigcap H \right)^g = \bigcap H^g = \bigcap H = N$$

Since g was arbitrary, we have $N \triangleleft G$.

[1B.8]

- (a) If $K, L \triangleleft G$ are such that G/K and G/L are π -groups, then since $G/(K \cap L)$ embeds in $(G/K) \times (G/L)$, we see $G/(K \cap L)$ is a π -group too. If N is the intersection of all normal subgroups of G with π -group quotients, then by induction G/N is a π -group, and N is the unique smallest normal subgroup where that is true, contained in all the others.

- (b) Let S be the set of π' elements. If $M \triangleleft G$ with G/M a π -group, and $x \in S$, then $\bar{x} \in G/M$ has π -order and π' -order, so has order 1. Since x was arbitrary, we see $S \subset M$. Since M was arbitrary, we have $S \subset N$, the intersection of all such M .

Let $K = \langle S \rangle$. Then we know $K \leq N$. We also know $K \triangleleft G$, since S is invariant under conjugation. If we can show G/K is a π -group, then by part (a) $N \leq K$, so that $K = N$. Choose a prime $p \notin \pi$. By [1B.5] there is a Sylow p -subgroup $P \leq G$ mapping to a Sylow p -subgroup of G/K . But $P \subset S$, so that $P \leq K$ and hence its image is trivial in G/K . Thus $|G/K|$ is not divisible by p . This shows G/K is a π -group.

1C

- [1C.1] Write $K = N_G(H)$. Since $P \leq H$, we see that $P \leq K$ is a Sylow p -subgroup of K . We also have $N_G(P) \leq H \leq K$, and thus $N_K(P) = N_G(P)$. Because $H \triangleleft K$ by definition, the Frattini argument shows

$$K = HN_K(P) = HN_G(P) = H$$

where the last equality follows because $N_G(P) \leq H$.

[1C.2]

- (a) By the Sylow development theorem, $P \leq S$ for some Sylow p -subgroup of G , so that $P \leq H \cap S$. Since $H \cap S$ is a p -subgroup of H , we must have equality (since P is a Sylow p -subgroup of H).
- (b) From the previous part, every Sylow p -subgroup of H can be written as $H \cap S$ for S a Sylow p -subgroup of G . Thus for every Sylow p -subgroup of H , there is a corresponding Sylow p -subgroup of G . We also can't have two Sylow p -subgroups P and Q of H corresponding to the same S , since then

$$P = H \cap S = Q$$

This implies $n_p(G) \geq n_p(H)$.

[1C.3]

- (a) If S is a Sylow p -subgroup of G , then every element of S is in X , so $\cup \text{Syl}_p(G) \subset X$. Conversely, if $g \in X$, then $\langle g \rangle$ is a p -subgroup, so contained in some Sylow p -subgroup of G . Because g was arbitrary, $X \subset \cup \text{Syl}_p(G)$.
- (b) Let S be a Sylow subgroup of G , and let it act on X by conjugation. If S fixes an element $g \in X$, then $\langle g \rangle S$ is a p -subgroup of G , so that $g \in S$. Thus the fixed points of the S -action are $Z(S) \subset X$. All other orbits have size divisible by p ; in other words,

$$|X| \equiv |Z(S)| \pmod{p}$$

But the same logic applied to S acting on S gives $|Z(S)| \equiv |S| \pmod{p}$, so that $|X| \equiv |S| \equiv 0 \pmod{p}$ as desired.

[1C.4] We know that $n_2(G) \in \{1, 3, 5, 15\}$. We consider the four cases below, with $P \leq G$ a Sylow 2-subgroup:

$[n_2(G) = 1]$ In this case, let $P \triangleleft G$ be a normal Sylow 2-subgroup. Then G/P has order 15, so again by Sylow's counting theorem it has a normal Sylow 5-subgroup. The preimage of that subgroup is an index 3 subgroup of G .

$[n_2(G) = 3]$ In this case $[G : N_G(P)] = n_2(P) = 3$.

$[n_2(G) = 5]$ In this case $[G : N_G(P)] = n_2(P) = 5$.

$[n_2(G) = 15]$ Since $15 \not\equiv 1 \pmod{4}$, there must be two Sylow 2-subgroups $P, Q \leq G$ with $P \cap Q$ of order 4. Then $P, Q \leq N_G(P \cap Q)$ by [1A.1]. Thus $N_G(P \cap Q)$ properly contains a Sylow 2-subgroup of G , and hence $[G : N_G(P \cap Q)] \in \{1, 3, 5\}$. We're done unless $N_G(P \cap Q) = G$. In that case $(P \cap Q \triangleleft G)$, note that $P \cap Q$ is contained in every Sylow 2-subgroup of G , and we consider $G/(P \cap Q)$ of order 30, with 15 Sylow 2-subgroups. Thus $G/(P \cap Q)$ has 15 elements of order 2. It can then not have 24 elements of order 5, so $n_5(G/(P \cap Q)) < 6$, and hence $G/(P \cap Q)$ has a normal Sylow 5-subgroup. The product of this with a Sylow 2-subgroup is a subgroup of order 10 in $G/(P \cap Q)$, which has a preimage of index 3 in G .

[1C.5] We must assume p is odd. Then the Sylow p -subgroups of A_{p+1} have order p . There are

$$\binom{p+1}{p} (p-1)! = \frac{(p+1)!}{p}$$

elements of order p in A_{p+1} . Since subgroups of order p intersect only in the identity, this means

$$\frac{(p+1)!}{p(p-1)} = n_p(A_{p+1}) = [A_{p+1} : N_G(P)]$$

Thus $|N_G(P)| = p(p-1)/2$ since $|A_{p+1}| = (p+1)!/2$.

[1C.6]

(a) From [1C.2], we know there's $P, Q \in \text{Syl}_p(G)$ such that $P \cap H$ is a Sylow p -subgroup of H , and $Q \cap K$ is a Sylow subgroup of K . Also $P = Q^g$ for some $g \in G$. If $g = hk$ (from $G = HK$), then $(P \cap H)^h = P^h \cap H$ is a Sylow subgroup of H (since it is an H -conjugate of a Sylow subgroup), and $(Q \cap K)^{k^{-1}} = P^h \cap K$ is a Sylow subgroup of K (since it is a K -conjugate of a Sylow subgroup). Thus $P^h \in \text{Syl}_p(G)$ satisfies the conditions of the problem.

(b) Let $|H| = p^a r$, $|K| = p^b c$, and $|G| = p^c t$. Then p^{a+b-c} must divide $|H \cap K|$. We have

$$|P \cap H| = p^a$$

$$|P \cap K| = p^b$$

$$|P \cap H \cap K| \leq p^{a+b-c}$$

And thus $|(P \cap H)(P \cap K)| \geq p^c$. Since it is contained in P (with $|P| = p^c$), we must have equality: $P = (P \cap H)(P \cap K)$.

[1C.7] Suppose $N_G(P) \neq G$, and let M be a maximal subgroup of G containing $N_G(P)$. Since $P \leq M$ we have $[G : M] = q$ with $q < p$ by hypothesis. But then

$$n_p(G) = [G : N_G(P)] = [G : M][M : N_G(P)] = qn_p(M) \equiv q \not\equiv 1 \pmod{p}$$

And this contradiction shows we must have $N_G(P) = G$.

[1C.8] Let X be the set of subgroups of order p^a in G . Let $P \in \text{Syl}_p(G)$ act on this set X by conjugation. By the orbit-stabilizer theorem, every non-trivial orbit has size divisible by p , and hence

$$|X| \equiv |X^P| \pmod{p}$$

where X^P is the union of the fixed points. But if $H \in X$ is fixed by P , then $P \leq N_G(H)$ and hence HP is a p -subgroup of G , so that $H \leq P$. We thus see that X^P are precisely the normal subgroups of order p^a in P .

Now let Y be all the subgroups of order p^a in P , and again let P act on Y . Then as before, $|Y| \equiv |Y^P| \pmod{p}$. But $Y^P = X^P$, and thus

$$|X| \equiv |X^P| = |Y^P| \equiv |Y| \pmod{p}$$

which was to be shown.

1D

[1D.1] Suppose P is a Sylow p -subgroup of H , contained (via Sylow development) in a Sylow p -subgroup $Q \leq G$, with $P < Q$. Then since normalizers grow in p -groups, we see that

$$P < N_Q(P) \leq N_G(P) \leq H$$

But $N_Q(P)$ is a p -subgroup, of H , properly containing P . This contradicts P being a Sylow p -subgroup of H . Thus $P = Q$ and P is a Sylow p -subgroup of G , implying

$$[G : H] = \frac{[G : P]}{[H : P]}$$

is not divisible by p (since $[G : P]$ isn't).

[1D.2] We assume p divides $|H|$, and show it does not divide $[G : H]$, which is equivalent to showing H contains a Sylow p -subgroup of G . By Cauchy's theorem there is an $x \in H$ with order p . Let $P \leq G$ be a Sylow p -subgroup containing x . Then we have $Z(P) \leq C_G(x) \leq H$ by hypothesis. Since $Z(P) \neq \{1\}$, there is an element $z \in Z(P)$ of order p . Again by hypothesis, $P \leq C_G(z) \leq H$, and we are done.

[1D.3]

(a) Let $1 < K \leq H$ and suppose $g \in G$ normalizes K . Then from

$$K \leq H \cap H^g$$

we see that $g \in H$. Since $g \in N_G(K)$ was arbitrary, we have $N_G(K) \leq H$.

(b) Let p be a prime dividing $|H|$. If $P \leq H$ is a Sylow p -subgroup of H , then from part (a) $N_G(P) \leq H$, and then from [1D.1] we see p does not divide $[G : H]$. So $|H|$ and $[G : H]$ are coprime, and H is a Hall subgroup.

[1D.4] First suppose $C_N(h) = \{1\}$ for all $1 \neq h \in H$. Let $g \in G$ be such that

$$1 \neq x \in H \cap H^g$$

If $g = yn$ with $n \in N$ and $y \in H$, then $H^g = H^n$, so we have $x, x^n \in H$. Then $x^{-1}x^n$ is in H , but also $x^{-1}x^n = n^{-x}n \in N$ since N is normal. Thus $x^{-1}x^n = 1$ and $x^n = x$. Then $n \in C_N(x) = \{1\}$ so that $g = y \in H$.

Conversely, suppose $1 \neq H \cap H^g$ implies $g \in H$. Let $1 \neq x \in H$, and suppose $x^n = x$ for $n \in N$. Then $x \in H \cap H^n$ and so $n \in H \cap N = \{1\}$. So $C_N(x)$ is trivial.

[1D.5] Suppose $H \cap H^g$ is non-trivial, and let Q be a non-trivial Sylow q -subgroup of $H \cap H^g$ for some prime q , so that Q and $Q^{g^{-1}}$ are both in H . By hypothesis, $N_G(Q) \leq H$ and also $N_G(Q^{g^{-1}}) = N_G(Q)^{g^{-1}}$ is in H . This says that $N_G(Q) \leq H \cap H^g$. By [1D.1], we see that Q is a Sylow q -subgroup of G . Thus Q and $Q^{g^{-1}}$ are Sylow subgroups of H , and are conjugate in H : say $Q^h = Q^{g^{-1}}$. This means $hg \in N_G(Q) \leq H$ and so $g \in H$. We have thus shown H is a Frobenius complement.

[1D.6] A subgroup of prime index is always maximal, since if $M \leq K \leq G$ then

$$[G : M] = [G : K][K : M]$$

but the left-hand side is prime, implying one of the factors on the right is 1. Conversely, suppose $M \leq G$ is a maximal subgroup and G is nilpotent. Then $M \triangleleft G$ so G/M is a group with no proper non-trivial subgroups (by the correspondence theorem). This means G/M is cyclic, and must be prime order, so that $[G : M]$ is prime.

[1D.7] Suppose $g \in \Phi(G)$. If $X \subset G$ is such that $\langle X \cup \{g\} \rangle = G$, then suppose $\langle X \rangle \neq G$. Then $\langle X \rangle$ is contained in some maximal subgroup $M \leq G$. But $g \in M$ as well, so $\langle X \cup \{g\} \rangle \leq M \neq G$, and this contradiction shows $\langle X \rangle = G$.

Conversely, suppose $g \in G$ is a "useless" element. If $M \leq G$ is a maximal subgroup not containing g , then $\langle M, g \rangle = G$ but $\langle M \rangle = M \neq G$. This contradicts g being useless, and so $g \in M$. Since M was an arbitrary maximal subgroup, $g \in \Phi(G)$.

[1D.8] If $M \leq G$ is maximal and G is nilpotent, then $M \triangleleft G$ and G/M has prime order by [1D.6]. In particular, G/M is Abelian, and $G' \leq M$. Since M was arbitrary, we have $G' \leq \Phi(G)$ and so $G/\Phi(G)$ is Abelian.

If G is a p -group, then like above G/M is of order p ; in particular, for all $x \in G$ we have $x^p \in M$. Since M was arbitrary, we have $x^p \in \Phi(G)$. But then in $G/\Phi(G)$, every element is such that $\bar{x}^p = 1$ and so $G/\Phi(G)$ is elementary Abelian.

Finally, if $N \triangleleft G$ for G a finite p -group and G/N is elementary Abelian, then the maximal subgroups of G/N are images of maximal subgroups of G containing N (by the correspondence theorem). Since the maximal subgroups of an elementary Abelian group are the hyperplanes, we see that all maximal subgroups of G/N intersect in the identity. If $\mathcal{M}$ is the set of maximal subgroups of G containing N , we then have

$$N = \bigcap_{M \in \mathcal{M}} M \geq \Phi(G)$$

Proving that $N \geq \Phi(G)$ and $\Phi(G)$ is the smallest normal subgroup with elementary Abelian quotient.

[1D.9] Suppose P has a single maximal subgroup $M \leq P$. Then for $x \in P \setminus M$, we must have $\langle x \rangle = P$ so that P is cyclic. So if P is noncyclic, then it has at least 2 maximal subgroups, and they each have index p ; call them M and N . Since $M \neq N$, we must have $[P : M \cap N] > p$ so that

$$[P : \Phi(P)] \geq [P : M \cap N] > p$$

and since $|P|$ is a power of p , we have $[P : \Phi(P)] \geq p^2$.

If $|P| = p^2$, then either P is cyclic or (from above) $\Phi(P) = \{1\}$. By the previous problem then $P = P/\Phi(P)$ is elementary Abelian.

[1D.10] Let $C = C_P(A)$ and suppose $A < C$. Since $C \triangleleft P$ we have by Lemma 1.23 a normal subgroup $K \triangleleft P$ with $[K : A] = p$ and $K \leq C$. This latter point implies $A \leq Z(K)$ so that $K/Z(K)$ has order dividing p , and is hence cyclic. But then $K = Z(K)$ is Abelian, contradicting the maximality of A .

So $C = A$, and the conjugation action of P on A induces an action on the $r := |A| - 1$ non-trivial elements of A . The kernel of this action is $C = A$, and so we get an injective homomorphism $P/A \rightarrow S_r$. Lagrange's theorem then implies $[P : A]$ divides $r!$.

[1D.11] We can rewrite the conclusion of the previous problem as $|P|$ divides $|A|!$. Let $P \leq G$ be a Sylow p -subgroup of G ; then a maximal normal Abelian subgroup $A \leq P$ has order at most n by hypothesis, so $|P|$ divides $|A|!$ (by the previous problem), which divides $n!$ since $|A| \leq n$.

Thus if $|G| = p^a q^b \cdots$, we see that $p^a, q^b, \dots$ all divide $n!$, and since they are coprime their product $|G|$ must divide $n!$ too.

[1D.12] This is part (b) of [1A.8].

[1D.13] By hypothesis G/Z has a central series:

$$1 < C_1 < C_2 < \cdots < C_n = G/Z$$

Let $Z_1 = Z$ and Z_{n+1} be the preimage of C_n in G for $n \geq 1$. Then for $n \geq 2$ we have $Z_{n+1}/Z_n = C_n/C_{n-1}$ is central in G/C_{n-1} , and $Z_1 \leq Z(G)$ is central in G . Thus the Z_k are a central series for G and G is nilpotent.

[1D.14] Let $P \leq \Phi(G)$ be a Sylow subgroup. The Frattini argument shows $G = N_G(P)\Phi(G) = N_G(P)$, where the last equality follows from [1D.7]. So $P \triangleleft G$, and so $P \triangleleft \Phi(G)$. Since all the Sylow subgroups of $\Phi(G)$ are normal, $\Phi(G)$ must be nilpotent.

[1D.15] Let us write $\bar{N}$ for the image of N in $G/\Phi(G)$.

Let $P \leq N$ be a Sylow subgroup such that $\bar{P}$ is a Sylow subgroup of $\bar{N}$ (via [1B.5]). Since $\bar{N}$ is nilpotent, its Sylows are normal (even characteristic) and hence $\bar{P} \triangleleft \bar{G}$, implying $P\Phi(G) \triangleleft G$. Since P is a Sylow subgroup of N contained in $P\Phi(G) \leq N$, the Frattini argument shows

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

with the last equality following from [1D.7]. Thus $P \triangleleft G$, and so $P \triangleleft N$. Since this works for all Sylow subgroups of N , we have shown N is nilpotent.

In particular, let $\Phi(G) \leq N \triangleleft G$ with N nilpotent. Then of course $\bar{N}$ is normal and nilpotent, so $\bar{N} \leq F(\bar{G})$, and in particular $\overline{F(G)} \leq F(\bar{G})$. Conversely, if $\bar{N} \triangleleft \bar{G}$ is nilpotent, then this problem proves N is nilpotent, so $N \leq F(G)$, meaning $\bar{N} \leq \overline{F(G)}$. Choosing $\bar{N} = F(\bar{G})$ we thus prove an equality

$$\overline{F(G)} = F(\bar{G})$$

[1D.16] Suppose $M \leq G$ is a maximal subgroup not containing $\Phi(N)$. Then $\Phi(N)M = G$ (it's a subgroup because $\Phi(N) \triangleleft G$). The Dedekind lemma then implies

$$N = G \cap N = \Phi(N)M \cap N = \Phi(N)(M \cap N)$$

By [1D.7] this means $N = M \cap N$ and so $\Phi(N) \leq N \leq M$. This contradiction shows $\Phi(N) \leq M$ for all maximal subgroups $M \leq G$, and so $\Phi(N) \leq \Phi(G)$.

[1D.17] By [1D.8] we have $N' \leq \Phi(N)$, and $\Phi(N) \leq \Phi(G)$ by the previous problem. So $G/\Phi(G)$ is a quotient of the nilpotent group G/N' , and is hence nilpotent. By [1D.15] G is nilpotent.

Note that if $G = S_3$ and $N = A_3$, then N is nilpotent, and G/N is Abelian (so also nilpotent). But S_3 is not nilpotent, since it doesn't have a normal Sylow 2-subgroup. So it is not true that N and G/N nilpotent imply G nilpotent.

[1D.18] Let us write $\bar{N}$ for $N/Z(G)$. Also note $Z(G)$ is normal and Abelian, so $Z(G) \leq F(G)$. Since $\overline{F(G)} \triangleleft \bar{G}$ is nilpotent, we have one containment: $\overline{F(G)} \leq F(\bar{G})$. Let $N \triangleleft G$ be such that $\bar{N} = F(\bar{G})$. We have left to show that N is nilpotent, since then $N \leq F(G)$. But $Z(G) \leq Z(N)$ and $N/Z(G)$ is nilpotent by hypothesis, so [1D.13] shows N is nilpotent.

[1D.19] We have

$$C \cap F \leq Z(C) \leq F(C)$$

Meanwhile $F(C) \triangleleft G$ is normal and nilpotent, so $F(C) \leq F \cap C$. In other words, $F(C) = Z(C)$. By the previous problem,

$$F(C/(C \cap F)) = F(C/Z(C)) = F(C)/Z(C) = \{1\}$$

Thus there are no non-trivial normal nilpotent subgroups of $C/(C \cap F)$.

1E

[1E.1] Suppose $n_q(G) > 1$; since $n_q(G)$ divides p^2 and is greater than $q > p$, it must be that $n_q(G) = p^2$. Then $p^2 \equiv 1 \pmod{q}$ so that q divides $(p-1)(p+1)$, and we must have $q = p+1$. Then $p = 2$ and $q = 3$, so $|G| = 36$.

Now if $|G| = 36$ and $n_3(G) > 1$, we have $n_3(G) = 4$, and since $4 \not\equiv 1 \pmod{9}$, there are two Sylow 3-subgroups $S, T \leq G$ with $N = S \cap T$ of order 3. The normalizer of N contains both S and T so must contain all 4 Sylow subgroups of G , implying both 9 and 4 divide $N_G(N)$ and thus $N \triangleleft G$. Because $n_3(G) > 1$, G/N cannot have a normal Sylow 3-subgroup, so counting elements shows it has a normal Sylow 2-subgroup, and thus there exists $P \leq G$ of order 4 with $PN \triangleleft G$. Thus PN contains all Sylow 2-subgroups of G .

If $n_2(G) > 1$, then from $n_2(G) = n_2(PN)$ we see that $n_2(G) = 3$, and thus $[G : N_G(P)] = 3$. The conjugation action on P induces a homomorphism $G \rightarrow S_3$ and so the kernel K must have size at least 6. We know $N \not\leq K$ since then $P \triangleleft PN \triangleleft G$ would imply $n_2(G) = 1$. We also know $P \not\leq K$ since P can't normalize other Sylow 2-subgroups, so it must be $|K| = 6$ and then K has a normal Sylow 3-subgroup M . Since M is characteristic in K we actually have $M \triangleleft G$. But then $MN \triangleleft G$ is order 9, contradicting $n_3(G) > 1$. So our assumption $n_2(G) > 1$ was wrong, and G has a normal Sylow 2-subgroup.

There do in fact exist groups of order 36 where $n_2 > 1$ or $n_3 > 1$. For respective examples, one can take $D_{18} \times C_2$ and $A_4 \times C_3$.

[1E.2] Suppose $n_r(G) > 1$. Since $n_r(G) \in \{1, p, q, pq\}$ and $r > q > p$, we must have $n_r(G) = pq$. There are thus $pq(r-1) = |G| - pq$ elements in all the Sylow r -subgroups of G . Now if $n_q(G) > 1$, from $n_q(G) \in \{1, p, r, pr\}$ we would have $n_q(G) \geq r$, accounting for at least $r(q-1) > pq$ elements in the Sylow q -subgroups of G , which is a contradiction. So $n_q(G) = 1$; let $Q \triangleleft G$ be the unique Sylow q -subgroup. Then in G/Q , of order pr , the Sylow r -subgroup must be normal. Thus there is a Sylow r -subgroup $R \leq G$ with $RQ \triangleleft G$. But in RQ we must have R normal as well, so $R \triangleleft G$ is our contradiction to $n_r(G) > 1$. Thus G has a normal Sylow r -subgroup.

[1E.3] Suppose $|G| = 315$ and is simple. Then $n_3(G) > 1$ and $n_3(G) \in \{1, 5, 7, 35\}$; the only one of these congruent to 1 modulo 3 is $n_3(G) = 7$. If $P \leq G$ is a Sylow 3-subgroup of G then,

we have $H := N_G(P) = 45$. Let $Q \leq H$ be a Sylow 5-subgroup. Since $n_5(H) \in \{1, 3, 9\}$, and only one of these is congruent to 1 modulo 5, we have $n_5(H) = 1$ and $Q \triangleleft H$. Thus $H \leq N_G(Q)$ and so

$$n_5(G) = [G : N_G(Q)] \leq [G : H] = 7$$

This means: $n_5(G) \leq 7$; $n_5(G)$ divides 63; and $n_5(G) \equiv 1 \pmod{5}$. The only possibility is $n_5(G) = 1$ so that $Q \triangleleft G$, contradicting simplicity. In fact we've shown more: any group of order 315 has either a normal Sylow 3-subgroup, or a normal Sylow 5-subgroup.

[1E.4] Let G have order 144 and be simple. Then $n_3(G) \in \{4, 16\}$. Since $|G| = 144$ does not divide $4!$, we have $n_3(G) = 16$. But $16 \not\equiv 1 \pmod{9}$ so there exists Sylow 3-subgroups $S, T \leq G$ with $N = S \cap T$ of order 3. Now $N_G(N)$ contains both S and T , so must contain at least 4 Sylow 3-subgroups, and thus $|N| \geq 36$. But then $[G : N] \leq 4$, and since $|G|$ doesn't divide $4!$, this contradicts G being simple.

[1E.5] Suppose G has order 336 and is simple. Then we know: $n_7(G) > 1$; $n_7(G)$ divides $2^4 3$; $n_7(G) \equiv 1 \pmod{7}$. The only possibility is $n_7(G) = 8$, and thus if $P \leq G$ is a Sylow 7-subgroup, then $|N_G(P)| = 42$. The conjugation action of G on P gives a homomorphism $\phi : G \rightarrow S_8$, which by simplicity must be injective and land in A_8 . But $\phi(P)$ is a Sylow 7-subgroup of A_8 , and by [1C.5] we then have

$$21 = |N_{A_8}(\phi(P))| \geq |N_{\phi(G)}(\phi(P))| = 42$$

This contradiction shows G cannot be simple.

[1E.6] Let $|G| = 180$ and assume G is simple. Then we know $n_3(G)$ is greater than 1, divides 20, and is congruent to 1 modulo 3. The only possibility is that $n_3(G) \in \{4, 10\}$. Since $|G|$ does not divide $4!$, we must then have $n_3(G) = 10$.

Let $S, T \leq G$ be two Sylow 3-subgroups of G . If $1 < D = S \cap T$, then $S, T \leq N_G(D)$ and so $n_3(N_G(D)) \geq 4$ and that means $|N_G(D)| \geq 36$ with $[G : N_G(D)] \leq 5$. Since $|G|$ does not divide $5!$, D cannot exist and so $S \cap T = \{1\}$. This means there are $10 * (9 - 1) = 80$ elements of order 3 or 9 in G .

Finally consider $n_5(G)$. As usual, it is larger than 1 and must divide 36, and is congruent to 1 modulo 5. The possibilities are then $n_5(G) = 6$ or $n_5(G) = 36$. The latter is ruled out because then there are $36 * (5 - 1) = 144$ elements of order 5, accounting for $144 + 80 > 180$ elements in G . But $n_5(G) = 6$ is also ruled out. To see this, let $P \leq G$ be a Sylow 5-subgroup, with $|N_G(P)| = 30$. There is an injective homomorphism $\phi : G \rightarrow A_6$ with $\phi(P)$ a Sylow 5-subgroup of A_6 . By [1C.5] we then have the contradiction

$$15 = |N_{A_6}(\phi(P))| \geq |N_{\phi(G)}(\phi(P))| = 30$$

Since there is no choice for $n_5(G)$, we've shown G cannot exist.

[1E.7] Let $|G| = 240$ and note $n_2(G) \in \{1, 3, 5, 15\}$. Since $|G|$ does not divide $5!$ (or $3!$) it must be that $n_2(G) = 15$ if G is simple. Since $15 \not\equiv 1 \pmod{4}$ there exists Sylow 2-subgroups

$S, T \leq G$ with $N = S \cap T$ of order 8. Then $S, T \leq N_G(N)$ and so $N_G(N)$ has at least 3 Sylow 2-subgroups, so $|N_G(N)| \geq 48$ and $[G : N_G(N)] \leq 5$. But again, $|G|$ does not divide $5!$ so we have that G cannot be simple.

[1E.8] Suppose $|G| = 252$ and G is simple. Then the only possibility for $n_7(G) > 1$, noting it must divide 36 and be congruent to 1 modulo 7, is $n_7(G) = 36$. There are thus $36(7 - 1)$ elements of order 7, and thus 36 elements of G with order coprime to 7.

Now suppose $S, T \leq G$ are Sylow 3-subgroups, with intersection $1 < D = S \cap T$. Then $S, T \leq N_G(D)$, so $N_G(D)$ has at least 4 Sylow 3-subgroups, and thus $N_G(D)$ has order at least 36. From the fact $n_3(N_G(D))$ divides 28 and is congruent to 1 modulo 3, we have $n_3(N_G(D)) \in \{4, 7, 28\}$. But

$$|N_G(D)| \geq 9 \cdot n_3(N_G(D))$$

and so $n_3(N_G(D)) > 4$ implies $[G : N_G(D)] \leq 4$, contradicting that $|G|$ does not divide $4!$ (and that $1 < D < G$ is not normal). It must then be that $n_3(N_G(D)) = 4$ and $|N_G(D)| = 36$. But then $N_G(D)$ consists of all elements of order coprime to 7 in G , which is a conjugate-invariant subset; in other words, $N_G(D) \triangleleft G$ and G is not simple. This contradiction shows D cannot exist.

Our final contradiction then is that every pair of Sylow 3-subgroups of G intersects trivially. Since $7(9 - 1) > 36$ we see that $n_3(G) \in \{1, 4\}$. But $|G|$ does not divide $4!$, and so G cannot be simple. Thus such a G does not exist.

1F

[1F.1] Let $m \in M$ and $n \in N$. From $[m, n] = m^{-1}m^n$ and $M^n = M$, we see that $[m, n] \in M$. Similarly, $[m, n] = n^{-m}n \in N$, and thus

$$[m, n] \in M \cap N = \{1\}$$

From $[m, n] = 1$ we deduce $mn = nm$. Since m and n were arbitrary, we see $M \leq C_G(N)$ and $N \leq C_G(M)$.

[1F.2] Choose Sylow p -subgroups $S, T \leq G$ with minimal intersection $D := S \cap T$ (in terms of size). Suppose $x \in Z(S) \cap Z(T)$. Then $x \in D$ is centralized by both S and T , so that $\langle x \rangle$ is normal in both S and T . Theorem 1.38 then shows $x \in O_p(G)$, so $x = 1$ by hypothesis. In other words, $Z(S) \cap Z(T) = \{1\}$.

[1F.3] Note that for $g \in G$ with $g = pn$ for $p \in P$ and $n \in N$, we have

$$p^g = p^{pn} = p^n$$

So conjugates of P by N are all the Sylow p -subgroups of G . Choose $x \in N$ such that $|P \cap P^x|$ is as small as possible, and let $D := P \cap P^x$. Then Theorem 1.38 applies here. Let $H \leq P$ be the kernel of the action of P on the orbit containing x . Clearly then $H \triangleleft P$.

But since H acts trivially on x , we must have $H \leq C_G(x)$ so that $H^x = H$ and $H \leq D$. Thus also $H = H^x \triangleleft P^x$, and so Theorem 1.38 implies $H \leq O_p(G)$. But $O_p(G) \triangleleft G$ and $O_p(G) \cap N = \{1\}$ by hypothesis, so that by [1F.1] $O_p(G)$ centralizes N . Since P acts faithfully on N , we must have $O_p(G) = 1$, and thus also $H = 1$. This shows P acts faithfully on the orbit of x .

1G

[1G.1] Let $M \triangleleft G$ be the Chermak-Delgado subgroup. As in the proof of Theorem 1.41, we have

$$\frac{|G|^2}{|A|^2} \geq \frac{|G|}{|A|} \frac{|G|}{|C_G(A)|} = \frac{|G|^2}{m_G(A)} \geq \frac{|G|^2}{m_G(M)} = \frac{|G|}{|M|} \frac{|G|}{|C_G(M)|} \geq \frac{|G|}{|M|}$$

By hypothesis, $[G : M] \geq [G : A]^2$; of course by definition $[G : M] \leq [G : A]^2$ and thus all the above inequalities must be equalities:

- From $|A|^2 = |A| \cdot |C_G(A)|$ and $A \leq C_G(A)$ we have $A = C_G(A)$.
- From $m_G(A) = m_G(M)$ we have $A \in \mathcal{L}(G)$.
- From $[G : C_G(M)] = 1$ and $M = C_G(M)$ we have $M \leq Z(G)$, while the reverse containment is always true, so $M = Z(G)$.

The last point shows $[G : Z(G)] = [G : M] = [G : A]^2$.

[1G.2] Let $M \in \mathcal{L}(G)$ be a maximal proper subgroup containing H . If M is normal in G , then we're done. If M is not normal, then there exists some $y \in G$ with $M^y \neq M$. But $m_G(M) = m_G(M^y)$, so that $M^y \in \mathcal{L}(G)$ and hence $H \leq M < MM^y \in \mathcal{L}(G)$, so by the choice of M we see $G = MM^y$. But then [1A.4] shows $G = M$, and that contradiction shows M must in fact be normal in G .

Note we've shown something stronger than the problem suggests: $H \leq M < G$ with M normal in G and $M \in \mathcal{L}(G)$.

[1G.3] If G is simple and Abelian, then there are only two subgroups of G , and $H = 1$ or $H = G$. So we may suppose that G is non-Abelian. Then the Chermak-Delgado subgroup $M \neq G$ so that $M = 1$, and $m_G(M) = |G|$. By hypothesis then $H \in \mathcal{L}(G)$. Now if $1 < H < G$ then the previous problem shows there exists $H \leq X \triangleleft G$ with $X \neq G$, and that contradicts simplicity of G . So $H = 1$ or $H = G$.

[1G.4] Suppose that $A \neq G$ and $[G : N] \geq [G : A]^2$ for all normal Abelian subgroups $N \triangleleft G$, and we will reach a contradiction. From [1G.1] we know that $A = C_G(A)$, that $A \in \mathcal{L}(G)$, and that $[G : Z(G)] = [G : A]^2$. If $N \triangleleft G$ is a normal Abelian subgroup, then so is $NZ(G)$, and

$$[G : NZ(G)] \leq [G : Z(G)] = [G : A]^2$$

Since $[G : NZ(G)] \geq [G : A]^2$ we must have $[G : NZ(G)] = [G : Z(G)]$ and hence $NZ(G) = Z(G)$; in other words, $N \leq Z(G)$ and all normal Abelian subgroups of G are contained in $Z(G)$.

As in the solution to [1G.2], choose a proper normal subgroup $M \in \mathcal{L}(G)$ containing A . Then $C_G(M) \triangleleft G$ and $C_G(M) \leq C_G(A) = A$, so $C_G(M)$ is a normal Abelian subgroup of G , and is thus contained in $Z(G)$. Since obviously $Z(G) \leq C_G(M)$ we have equality: $C_G(M) = Z(G)$. But then

$$G > M = C_G(C_G(M)) = C_G(Z(G)) = G$$

is our contradiction.

2A

[2A.1] We proceed by induction on the subnormal depth of H , the case of zero depth (so $H = G$) being obvious (since in that case $O_\pi(G) = G$). Otherwise, consider a normal series

$$H = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_k = G$$

By induction, $H \leq O_\pi(H_{k-1})$. But $H_{k-1} \triangleleft G$, and thus $O_\pi(H_{k-1}) \triangleleft G$, so that by definition $O_\pi(H_{k-1}) \leq O_\pi(G)$. Thus we have $H \leq O_\pi(G)$.

Now if H, K are two subnormal π -subgroups of G , we know that $\langle H, K \rangle \triangleleft\triangleleft G$, and since this problem shows $H, K \leq O_\pi(G)$, we see $\langle H, K \rangle \leq O_\pi(G)$, so that $\langle H, K \rangle$ is a π -subgroup.

[2A.2] We proceed by induction on the subnormal depth of H , the case of zero depth (so $H = G$) being obvious. Otherwise, consider a normal series

$$H = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_k = G$$

By induction (since $[H_{k-1} : H]$ divides $[G : H]$) we have $O^\pi(H_{k-1}) \leq H$. But $H_{k-1} \triangleleft G$, so $O^\pi(H_{k-1}) \triangleleft G$, and

$$[G : O^\pi(H_{k-1})] = [G : H_{k-1}][H_{k-1} : O^\pi(H_{k-1})]$$

is a product of two π -numbers. Thus $O^\pi(G) \leq O^\pi(H_{k-1})$ and thus $O^\pi(G)$ is contained in H .

[2A.3]

- (a) Let $[G : H]$ be a π -number (here π contains every prime dividing $[G : H]$). Then from [2A.2] we see that $O^\pi(G) \leq H$. Meanwhile $|K|$ and $|G/O^\pi(G)|$ are relatively prime, so the image of K in the quotient is trivial, so $K \leq O^\pi(G)$. Thus $K \leq H$.

- (b) Let $|K|$ be a π -number (here π contains every prime dividing $|K|$). Then from [2A.1] we see that $K \leq O_\pi(G)$. We have

$$\frac{|HO_\pi(G)|}{|H|} = \frac{|O_\pi(G)|}{|H \cap O_\pi(G)|}$$

The left-hand side is a π' -number, while the right-hand side is a π -number. Hence both sides are 1, so that $O_\pi(G) \leq H$. Thus $K \leq H$.

[2A.4] Nothing is lost assuming $G = HS$. Since $S \cap H \triangleleft\triangleleft S$ and S is simple, we must have $S \cap H = S$ or $S \cap H = \{1\}$. The first case implies $S \leq H \leq N_G(H)$, so we can restrict to $S \cap H$ being trivial.

Since $H < HS$ and H is subnormal, there is a proper normal subgroup $N \triangleleft HS$ containing H . Then

$$N = HS \cap N = H(S \cap N)$$

Now $S \cap N \triangleleft S$, so it is either $\{1\}$ or S . In the first case, $N = H$, and in the second case, $N = HS$, which we've excluded. So $H = N \triangleleft HS$ so that $S \leq N_G(H)$, and we're done.

[2A.5]

- (a) For any subset $\mathcal{Y} \subset \mathcal{X}$, let $P_{\mathcal{Y}}$ be the product

$$P_{\mathcal{Y}} := \prod_{M \in \mathcal{Y}} M$$

Since $P_{\mathcal{X}} = N$, we can choose a minimal subset $\mathcal{Z} \subset \mathcal{X}$ with $P_{\mathcal{Z}} = N$. We will show this product is direct. Let $M \in \mathcal{Z}$ and define $\mathcal{M} = \mathcal{Z} \setminus M$. Then $P_{\mathcal{M}} \cap M \triangleleft G$, and since M is a minimal normal subgroup of G , we must have this intersection is either $\{1\}$ or M . The first case is what we want, to show the product is direct. The second case cannot happen, since then

$$P_{\mathcal{M}} = MP_{\mathcal{M}} = P_{\mathcal{Z}} = N$$

contradicting the minimality of $\mathcal{Z}$.

- (b) Let $K \triangleleft N$ be a minimal normal subgroup of N , and let $H \triangleleft K$ be a normal subgroup of K . Then $H \triangleleft\triangleleft G$ and so every element of $\mathcal{X}$ normalizes K by Theorem 2.6. This means $H \triangleleft N$, and since K is a minimal normal subgroup, we have $H = \{1\}$ or $H = K$, so that K is simple.
- (c) Let M be the socle of N . By part (a), M is the direct product of some subset of minimal normal subgroups of N . By part (b), every minimal normal subgroup of N is a simple group. Thus we know M is a direct product of simple groups, and it is enough then to show $M = N$. For $X \in \mathcal{X}$, we have $X \triangleleft N$, so that $1 < X \cap M$. But $M \triangleleft G$ and X is a minimal normal subgroup of G , so $X \leq M$. Since $X \in \mathcal{X}$ was arbitrary, we have $N \leq M$, as desired.

The case of $|\mathcal{X}| = 1$ shows a minimal normal subgroup of G is a product of simple groups. The case where $\mathcal{X}$ is all minimal normal subgroups of G shows the socle of G is a product of simple groups.

[2A.6] Let $1 < M \triangleleft G$ be non-Abelian, with $M \leq N$. If $X \in \mathcal{X}$, then either $M \cap X = \{1\}$ or $X \leq M$. Since the latter case is what we want, we assume that the first case happens for all $X \in \mathcal{X}$ and reach a contradiction. Since M and X are normal subgroups of G , and they intersect trivially, we have $X \leq C_G(M)$. Since this supposedly holds for all elements of $\mathcal{X}$, we have $N \leq C_G(M)$. But $M \leq N$, so that $M \leq Z(N)$, and this contradicts $M \neq 1$ and M being non-Abelian. Thus some member of $\mathcal{X}$ is contained in M .

[2A.7] If $S = G$ we're done, so we assume $S < G$, and we proceed by induction on $|G|$, the case $|G| = 1$ being trivial. Otherwise by induction we have S^H is a minimal normal subgroup of H for all $H < G$ with $S \leq H$. In particular, S is in the socle of every proper subgroup of G containing S . Specifically, S is in the socle of S^G . But $\text{Soc}(S^G) \triangleleft G$, so that $S^G \leq \text{Soc}(S^G)$, and we have equality: S^G is equal to its own socle. By Theorem 2.6 we see that $S \triangleleft S^G$. Thus for any $x \in G$, we have

$$S^x \triangleleft (S^G)^x = S^G$$

Let $\mathcal{X} = \{S^x \mid x \in G\}$, so that S^G is the product of elements of $\mathcal{X}$. Let $N \leq S^G$ be a normal subgroup of G . We show $N = 1$ or $N = S^G$, finishing the proof $S^G \triangleleft G$ is minimal normal. Now if N is non-Abelian, then by [2A.6] we see there's some $S^x \leq N$. But then by normality every conjugate of S is contained in N , so $S^G \leq N$ and we have $N = S^G$. If instead N is Abelian, then $N \cap S^x < S^x$ is a proper normal subgroup, so $N \cap S^x = \{1\}$. But N and S^x are normal subgroups of S^G , so we see $S^x \leq C_G(N)$. This holds for all $x \in G$, so $N \leq Z(S^G)$. We show $N = 1$ via [2A.5], since that problem gives $\{g_1, \dots, g_k\} \subset G$ with

$$\begin{aligned} S^G &= \prod_{i=1}^k S^{g_i} \\ Z(S^G) &= \prod_{i=1}^k Z(S^{g_i}) \\ &= \{1\} \end{aligned}$$

where the last equality follows since S is non-Abelian simple, so it has trivial center.

[2A.8] We proceed by induction on $|G|$. If $S, T \leq H < G$, then the inductive hypothesis shows S and T commute elementwise. If we suppose no such H exists, then by the previous problem S^G and T^G are minimal normal subgroups of G , and they must be proper since S (and T) are proper subnormal subgroups. By our assumption $S^G \neq T^G$, so they have trivial intersection, and hence commute elementwise. But then we're done, since $S \leq S^G$ and $T \leq T^G$.

[2A.9] We lose nothing working in $K = HO_\pi(G)$. Then $[K : H]$ is a π -number, so by [2A.2] we

have $O^\pi(K) \leq H$. But $H/O^\pi(K)$ is a π -group, so by hypothesis it must be the trivial group, so $H = O^\pi(K)$. Then $H \triangleleft K$ and we're done.

[2A.10] There's nothing to prove if $H = G$, so we assume throughout $H < G$. First suppose H is subnormal in G , and let $K \leq G$ be such that H is conjugate to K in $\langle H, K \rangle$. We write a normal series

$$H = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_k = G$$

Since K is conjugate to H , we have $K \leq H_{k-1}$ so that $\langle H, K \rangle \leq H_{k-1}$. But then H and K are conjugate in H_{k-1} , so both lie in $H_{k-2} \triangleleft H_{k-1}$. Continuing this way, we see that after finitely many steps we have $K \leq H_0 = H$, so that $K = H$.

Conversely, assume that H is only strongly conjugate to itself. We proceed by induction on $|G|$, so that for every proper subgroup $K < G$ containing H , we have $H \triangleleft\triangleleft K$. If H is not subnormal in G , then the Zipper lemma gives a unique maximal subgroup $M < G$ containing H . Now if $x \in G$ is such that $H^x \neq H$, then we cannot have $\langle H, H^x \rangle = G$ (since H is not strongly conjugate to H^x), and thus $H \leq \langle H, H^x \rangle < G$ shows $H^x \leq M$. Since this is true for all $x \in G$, we have $H^G \leq M$, so that our inductive hypothesis gives us

$$H \triangleleft\triangleleft H^G \triangleleft G$$

so that $H \triangleleft\triangleleft G$, a contradiction establishing H is subnormal in G .

2B

[2B.1] We work by induction on $|G|$. Note that, via the inductive hypothesis, for every proper subgroup $K < G$ containing H , we have $H \triangleleft\triangleleft K$. If H is not subnormal in G , then the Zipper lemma applies, and we have H contained in a unique maximal subgroup $M < G$. We show this leads to a contradiction. First note that saying H is not subnormal in G implies G is not nilpotent.

Choose $g \in G$ with $H^g \neq H$. If $H^g \not\leq M$, then $\langle H, H^g \rangle = G$. Since G is not nilpotent, we must have $HH^g \leq G$, so that $HH^g = \langle H, H^g \rangle = G$. Then $H = G$, which is absurd. Thus we must always have $H^g \leq M$. Then $H^G \leq M$, so our inductive hypothesis shows

$$H \triangleleft\triangleleft H^G \triangleleft G$$

and this contradiction shows H is subnormal in G .

[2B.2] (a) Let $C \leq D$ be the cyclic subgroup of order n . Since n is odd, C has no involutions. Meanwhile, $D \setminus C$ is all involutions, so D has $|D| - |C| = n$ involutions. Let $C = \langle c \rangle$

and $D = \langle s, c \rangle$ with s an involution. Then every element of $D \setminus C$ is given by sc^k for $0 \leq k < n$. We have

$$(sc^m)sc^k(sc^m) = sc^m(c^{-k}s^2c^m) = sc^{2m-k}$$

Since n is odd, we can always solve $2m \equiv k + r \pmod{n}$, so that sc^k is conjugate to sc^r for any $0 \leq r < n$, and thus $D \setminus C$ is one conjugacy class.

- (b) Let $C \leq D$ be the cyclic subgroup of order n . Then C has a unique involution, while $D \setminus C$ has $|D| - |C| = n$ involutions, so D has $n + 1$ involutions. Let $t \in C$ be the unique involution. Then $\langle t \rangle$ is characteristic in C , so $\langle t \rangle \triangleleft D$, and t is its own conjugacy class. Let $D = \langle s, c \rangle$ where $s \in D \setminus C$ and $C = \langle c \rangle$. Then note that, as above,

$$\begin{aligned} (sc^m)sc^k(sc^m) &= sc^{2m-k} \\ c^{-m}(sc^k)c^m &= sc^{2m+k} \end{aligned}$$

But $2m \equiv r \pm k \pmod{n}$ is only solvable when $r + k$ is even, since n is even. This shows $D \setminus C$ is two conjugacy classes, represented by sc^k for k odd and even. These conjugacy classes each have size $\frac{1}{2}|D \setminus C| = n/2$.

[2B.3] Let $D = \langle s, t \rangle \leq G$ be a dihedral subgroup. If $|D| = 2n$ for n odd, then by part (a) of the previous problem, we would have s conjugate to t in D , hence in G . So we must have n even, so that D has a central involution $z \in D$ by part (b) of the previous problem. Then z commutes with s and t , but is not equal to either of them, since both live in $D \setminus \langle z \rangle$.

[2B.4] Suppose $s, t \in G$ are non-conjugate involutions, with $s \in P$ and $t \in Q$ for Sylow 2-subgroups $P, Q \leq G$. We can assume $P \neq Q$ by replacing t with t^g for some $g \notin N_G(P)$. This works because if s is conjugate to t^g , then it's conjugate to t . By the previous problem, there's an involution $z \in G$ commuting with both s and t . Then $\langle s, z \rangle$ is a 2-group (of order 4), so by hypothesis it's contained in the Sylow subgroup containing s , namely P . Similarly, $\langle t, z \rangle$ is contained in the Sylow subgroup containing t , namely Q . $1 \neq z$ is then contained in both P and Q , which is our contradiction. Thus all involutions are conjugate.

[2B.5]

[1 $\implies$ 2] An element of $G \setminus B$ looks like bt for $b \in B$. Then, by the assumption in (1), we have

$$(bt)^2 = b(tbt) = b(t^{-1}bt) = b(b^{-1}) = 1$$

so that bt is an involution. Since this was an arbitrary element, every element of $G \setminus B$ is an involution.

[2 $\implies$ 3] Let $t \in G \setminus B$. (2) already gives us that t is an involution. Let $b \in B$, and note that bt is also an involution by (2). Thus

$$1 = (bt)^2 = b(tbt) = bb^t$$

showing that $b^t = b^{-1}$. Since b was arbitrary, (3) is established.

[3 $\implies$ 1] Trivial.

If any of these conditions hold, let $t \in G \setminus B$ be an involution inverting every element of B via conjugation. Then for $a, b \in B$ we have

$$b^{-1}a^{-1} = (ab)^{-1} = (ab)^t = a^tb^t = a^{-1}b^{-1}$$

And this rearranges to $ba = ab$. Since $a, b \in B$ were arbitrary, this shows B is Abelian.

[2B.6] We note that the problem can be restated as: G has a normal Sylow p -subgroup if and only if $\langle x, x^g \rangle$ is a p -subgroup for all x of p -power order.

Suppose first that G has a normal Sylow p -subgroup P , and let $x, y \in G$ be conjugate elements of order p^a . Then both are contained in the unique Sylow subgroup P , so $\langle x, y \rangle$ is a p -group.

Conversely, suppose $\langle x, x^g \rangle$ is a p -group for any $x \in P$, with $P \leq G$ a Sylow p -subgroup, and any $g \in G$ (this is equivalent to our converse, since all p -power order elements of G are conjugate into P). Then if $X = \langle x \rangle$, we see from Baer's theorem that $X \triangleleft\triangleleft G$. Since X is trivially nilpotent, we have $X \leq F(G)$. But then since X is a p -group, we have $X \leq O_p(G)$. Since $x \in P$ was arbitrary, we have $P \leq O_p(G)$, so that $P = O_p(G)$ is normal in G .

2C

[2C.1]

- (a) Let $1 < K \triangleleft G$ be a non-trivial normal subgroup of the N -group G . If p is a prime dividing $|K|$, and $1 < P \leq K$ is a Sylow p -subgroup of K , then the Frattini argument shows $G = N_G(P)K$. Thus G/K is the homomorphic image of $N_G(P)$, which is solvable by hypothesis. Hence G/K is solvable.
- (b) Now let G be a non-solvable N -group. If $S, N \triangleleft G$ are two distinct minimal normal subgroups, then the natural homomorphism $G \rightarrow (G/S) \times (G/N)$ is injective because $S \cap N = \{1\}$. By part (a), the group on the right is solvable, so this shows G is solvable. This contradiction shows G does not have two distinct minimal normal subgroups. We let $S \triangleleft G$ be the unique minimal normal subgroup.

Since G/S is solvable and G is not, we must have that S is non-solvable. If $P \leq S$ is a non-trivial p -subgroup for some prime p , then $N_S(P) \leq N_G(P)$ is solvable. Thus S is a non-solvable N -group as well. By what's just been proved, S has a unique minimal normal subgroup $N \triangleleft S$. But then $N \triangleleft G$, and by minimality we must have $N = S$. This implies that S is simple.

2D

[2D.1]

- (a) Note that $F(G) \cap N \leq F(N) = \{1\}$, and thus $F(G) \leq C_G(N)$. This shows that $A \cap F(G) \leq C_A(N) = \{1\}$. By Corollary 2.19, we must have

$$|A| < [G : A] \leq |N|$$

- (b) Suppose $A \cap F(G) > 1$, and let p be a prime dividing $|A \cap F(G)|$. This means that $O_p(G) > 1$, but the coprimeness hypothesis shows $N \cap O_p(G) = \{1\}$, so that $O_p(G)$ is contained in $C_G(N)$. Then we have

$$A \cap F(G) \leq O_p(G) \leq C_G(N)$$

implying $C_A(N) > 1$. So our hypothesis shows $A \cap F(G) = \{1\}$, and thus by Corollary 2.19 we have

$$|A| < [G : A] \leq |N|$$

[2D.2]

Suppose for contradiction that $|A| \geq [G : A] = |N|$. Then Lucchini's theorem shows there is a normal subgroup $1 < K \triangleleft G$ contained in A . But then $K \cap N = \{1\}$, so that K centralizes N . In other words, $1 < K \leq C_A(N)$, and this contradicts our hypotheses. Thus $|A| < |N|$.

3A

[3A.1]

- (a) Let $|C| = n$. We define the map $\sigma : C \rightarrow C$ via

$$\sigma(c^r) = (c^{-1}z)^r = c^{-r}z^r$$

where the last equality relies on C being Abelian. We can see this is a homomorphism via

$$\sigma(c^r c^s) = c^{-r-s} z^{r+s} = c^{-r} z^r c^{-s} z^s = \sigma(c^r) \sigma(c^s)$$

It is also injective, since $c^{-r} z^r = 1$ is equivalent to $c^r = z^r$, implying $n/2$ divides r , meaning that $z^r = 1$, so that $c^r = 1$. But C is finite, so σ is surjective as well, and is thus an automorphism of C . It is unique since automorphisms of C are determined by what they do to $c \in C$.

(b) Consider the element $c^r\sigma \in S$. We compute

$$(c^r\sigma)^2 = c^r(\sigma c^r\sigma) = c^r c^{-r} z^r = z^r$$

where we've used that $\sigma c^r\sigma = \sigma(c^r)$, which we computed in part (a). Thus if r is even, we see that $c^r\sigma$ has order 2. Meanwhile, if r is odd, we have $(c^r\sigma)^2 = z$. Since $z^2 = 1$, it must be that $c^r\sigma$ has order 4 when r is odd. Thus $S \setminus C$ consists of n elements, half of them order 2, half of them order 4.

(c) For $c^r\sigma \in S \setminus C$, we compute its centralizer. First note that $\sigma(c^m) = c^m$ implies that $c^{2m} = z^m$, meaning n divides $4m$. This implies m is even, so that $c^{2m} = 1$ and thus $c^m \in \{1, z\}$. Since $(c^r\sigma)^{-1}c^m(c^r\sigma) = \sigma(c^m)$, we've shown

$$C_S(c^r\sigma) \cap C = \{1, z\}$$

But $[C_S(c^r\sigma) : C_S(c^r\sigma) \cap C] = 2$; it is bounded below by 2 since $c^r\sigma \in C_S(c^r\sigma) \setminus C$, and bounded above by 2 since $[S : C] = 2$. We thus know that $|C_S(c^r\sigma)| = 4$, so that it has $|S|/4 = n/2$ conjugates. All these conjugates live in $S \setminus C$, where there are at most $n/2$ conjugates by part (b). So the two sets in part (b) are actually full conjugacy classes in S .

[3A.2] Let $B \leq C$ be the subgroup of index 2. As shown in part (b) of the previous problem, the elements of order 4 in $S \setminus C$ all look like $c^r\sigma$ for r odd. All of these live in the same coset $B(c\sigma)$, since

$$(c^r\sigma)(c\sigma)^{-1} = c^{r-1}$$

and $r-1$ is even. We let $Q = B \sqcup B(c\sigma)$. We show it is closed under products; that shows $Q \leq S$ since $1 \in B \leq Q$ and Q is finite, so eventually iterated products become inverses. Now of course B is closed under products, and we otherwise compute

$$\begin{aligned} (c^{2k})(c^r\sigma) &= c^{2k+r}\sigma \in Q & (r \text{ is odd}) \\ (c^r\sigma)(c^s\sigma) &= c^{r-s}z^s \in Q & (r-s \text{ is even}) \end{aligned}$$

Thus $Q \leq S$ is a subgroup of order $2|B| = |C| = n$. Every element of $Q \setminus B$ has order 4, and B has a unique involution, so Q has a unique involution.

[3A.3] We write C_k for the cyclic group of order k . Since $\text{Aut}(C_p) \cong C_{p-1}$, we know there's an element $\sigma \in \text{Aut}(C_p)$ of order m . We let

$$G := C_p \rtimes \langle \sigma \rangle$$

Then $|G| = pm$, and $P := C_p$ is a normal Sylow p -subgroup of order p in G . Also $G/P \cong \langle \sigma \rangle$ is cyclic of order m . Now if σ^k fixed any non-trivial element of P , it would fix all of P (since P is simple), and hence (as an automorphism) we would have σ^k acting trivially, so that $\sigma^k = 1$. This shows any element of $G \setminus P$ cannot be in $Z(G)$. Meanwhile, since $x^\sigma \neq x$ for non-trivial $x \in P$, we see that $Z(G) \cap P = \{1\}$, and thus $Z(G)$ is trivial.

[3A.4] Let F be the field of q elements, and write $H := F^*$, the set of non-zero elements of F .

Then H acts on F (as an additive group) via multiplication, and we can form the semidirect product

$$G := F \rtimes H$$

[Note: this is an action because multiplication is commutative, and it is an action by automorphisms because multiplication distributes over addition.]

Thus $|G| = q(q-1)$ and $F \triangleleft G$. As an additive group, F is elementary Abelian. Since $|G|/|F|$ is not divisible by p , we see that F is the normal Sylow p -subgroup of G . To finish the problem then, we need to show all non-trivial elements of F are conjugate in G . But let $a, b \in F^*$ and write $h = b/a$. Then $a^h = b$ in G , and we're done.

[3A.5] We write $\widehat{G}$ for the group G acting on itself via (inner) automorphisms. In the semidirect product, this means $\widehat{g}^{-1}h\widehat{g} = h^g = g^{-1}hg$. Now we define a bijection $\phi : G \times G \rightarrow G \rtimes \widehat{G}$ via

$$\begin{aligned}\phi(a, b) &= ab^{-1}\widehat{b} \\ \phi^{-1}(cd, d) &= (cd, d)\end{aligned}$$

We show this preserves products, so that it's an isomorphism.

$$\phi(ac, bd) = ac(bd)^{-1}\widehat{bd} = acd^{-1}b^{-1}\widehat{bd}$$

Meanwhile,

$$\phi(a, b)\phi(c, d) = ab^{-1}\widehat{b}cd^{-1}\widehat{d} = ab^{-1}(\widehat{bcd}^{-1}\widehat{b}^{-1})\widehat{bd} = ab^{-1}(bcd^{-1}b^{-1})\widehat{bd} = acd^{-1}b^{-1}\widehat{bd}$$

[3A.6] Note that P is a Sylow subgroup of the semidirect product $S := G \rtimes P$. Choose $g \in G$ such that $P \cap P^g$ is minimal, so that by Brodkey's theorem $O_p(S)$ is the largest subgroup in $P \cap P^g$ normal in both P and P^g . But $O_p(S) \cap G = \{1\}$, so that $O_p(G) \leq C_S(G) \cap P$; since P acts faithfully on G , we must have $O_p(S) = \{1\}$.

Consider the action of P on the orbit of g , and let $A \leq P$ be the subgroup that acts trivially on this orbit. Then $g \in C_S(A)$ so that $A \leq P \cap P^g$. Also for $x \in P$ we have A^x acts trivially on the orbit of g^x , which is the orbit of g , hence $A^x = A$. Thus $\langle P, g \rangle \leq N_S(A)$, so that A is normal in both P and P^g . By the first paragraph, we have

$$A \leq O_p(G) = \{1\}$$

so that P acts faithfully on the orbit of g .

[3A.7] Let $A = \langle \sigma \rangle$ and suppose

$$|A| = \prod_{i=1}^m p_i^{\alpha_i}$$

where the p_i are primes and each $\alpha_i > 0$. Let $a_i \in A$ be an element of order p_i . Note that if $1 < B \leq A$, then some p_i divides $|B|$, and since A has a unique subgroup of order p_i , it

must be that $a_i \in B$. In particular, for every non-trivial subgroup $1 < B \leq A$, we always have

$$B \cap \{a_1, \dots, a_m\} \neq \emptyset$$

Now define subgroups $G_i \leq G$ as $G_i = C_G(a_i)$. These subgroups are proper since $a_i \neq 1$. Note that if $g \in G$ is such that $g \notin \cup G_i$, then we have $a_i \notin C_A(g)$ for all i , so by the above we have $C_A(g) = \{1\}$. In particular, the orbit of g is a regular orbit. So this problem is solved if we show such a $g \in G$ exists whenever $i \leq 2$.

In the case $i = 1$, such a g clearly exists since $G_1 < G$. In the case $i = 2$, we can construct such a g . To do this, note that we can assume neither subgroup is contained in the other, since that case is easy. Let $x \in G_1 \setminus G_2$ and $y \in G_2 \setminus G_1$. Then we must have $xy \notin G_1 \cup G_2$.

[3A.8]

- (a) Write $C = C_p \times C_q \times C_r$. We can define an automorphism α_p that acts on each factor separately: as the identity on C_p , and as inversion on the other 2 factors. Clearly α_p is unique, since automorphisms of C are determined by what they do to generators. We can of course similarly define α_q and α_r .
- (b) Note that $\alpha_p \alpha_q \equiv \alpha_r$. Since each has order 2, we see that $K := \langle \alpha_p, \alpha_q \rangle \leq \text{Aut}(C)$ is a dihedral group of order $2|\alpha_r| = 4$; that is, $K = \{1, \alpha_p, \alpha_q, \alpha_r\}$ is an elementary Abelian group of order 4.
- (c) Define $G := C \rtimes K$, and let $c \in C$ be a generator, and σ the inner automorphism that conjugates by c . Of course σ fixes every element of $C \leq G$. Let $c^k \neq 1$ be an element contained in C_p . Then

$$\sigma^k(\alpha_p) = c^{-k} \alpha_p c^k = c^{-k} (\alpha_p c^k \alpha_p) \alpha_p = c^{-k} \alpha_p (c^k) \alpha_p = c^{-k} c^k \alpha_p = \alpha_p$$

and thus σ^k fixes α_p . This is thus true for every element in the coset $C\alpha_p$. Similarly, there is a non-trivial element in $\langle \sigma \rangle$ that fixes every element of the coset $C\alpha_q$, and another for the coset $C\alpha_r$. Thus every element of G has a non-trivial centralizer in $\langle \sigma \rangle$, so that σ has no regular orbit.

In the context of the previous solution, what's going on here is that G is the union of three subgroups $\langle C, \alpha_p \rangle$, $\langle C, \alpha_q \rangle$, and $\langle C, \alpha_r \rangle$. Each of these is fixed by an element of (different) prime order in $\langle \sigma \rangle$, and so we have no regular orbit.

[3A.9]

- (a) Of course, a constant function is invariant under the action of G , since

$$f^g(\alpha) = f(\alpha \cdot g^{-1}) = f(\alpha)$$

Conversely, if $f : \Omega \rightarrow H$ is invariant under G , then for $\alpha, \beta \in \Omega$ there exists $g \in G$ with $\alpha \cdot g = \beta$, and hence

$$f(\alpha) = f(\beta \cdot g^{-1}) = f^g(\beta) = f(\beta)$$

Since α and β were arbitrary, f is constant.

- (b) We must assume H is non-trivial, so that there exists $h \neq 1$ in H . For $C \leq G$, define $f \in B$ as

$$f(g) = \begin{cases} 1 & g \in C \\ h & g \notin C \end{cases}$$

Then if $c \in C$, right multiplication by C leaves the two subsets C and $G \setminus C$ invariant. The same is true for $c^{-1} \in C$, and thus $f^c \equiv f$. However, if $g \in G \setminus C$, then

$$f(g) = h \neq 1 = f(gg^{-1}) = f^g(g)$$

Thus $C_G(b) = C$.

- [3A.10] Let $G := C_p \wr H$, and let A be the base group (an elementary Abelian p -group of order $p^{|H|}$). Thus $A \triangleleft G$, $G = AH$, and $A \cap H = \{1\}$. So what's left is to show $C_G(A) = A$. Obviously $A \leq C_G(A)$, so from $G = AH$ it's enough to show no non-trivial $h \in H$ centralizes A . But this is clear: let $f : H \rightarrow C_p$ be such that $f(x) = 1$ if and only if $x = 1$. Then

$$f^h(1) = f(h^{-1}) \neq 1 = f(1)$$

so that $f^h \neq f$, and $f \in A$ implies $h \notin C_G(A)$.

3B

- [3B.1] Let G be solvable, and we work via induction on $|G|$ to show all maximal subgroups have prime-power index. Assuming $|G| > 1$, let $M \leq G$ be a maximal subgroup and let $N \triangleleft G$ be a minimal normal subgroup, which is elementary Abelian for some prime p . If $N \leq M$, then by induction $[G/N : M/N] = [G : M]$ is prime-power order. Otherwise, we must have $G = MN$. Since $M \cap N \triangleleft M$ and also $M \cap N \triangleleft N$ (because N is Abelian), we have $M \cap N \triangleleft G$, so that by minimality we have $M \cap N = \{1\}$. Then $G = N \rtimes M$ and $[G : M] = |N| = p^a$ is a prime power, and we're done.

- [3B.2] We assume $r > 0$. Since N_k/N_{k-1} is abelian, we always have $[N_k, N_k] \leq N_{k-1}$. Specifically, we have $[N_r, N_r] = [G, G] = G^{(1)} \leq N_{r-1}$. But then we have

$$G^{(2)} = [G^{(1)}, G^{(1)}] \leq [N_{r-1}, N_{r-1}] \leq N_{r-2}$$

And continuing this way, we see that $G^{(r)} \leq N_0 = \{1\}$, so that G is solvable.

- [3B.3] First we assume G is solvable. Then by Lemma 3.10 each N_i/N_{i-1} is solvable. Since these groups are simple, they must be Abelian (otherwise simplicity implies N_i/N_{i-1} has no normal Abelian subgroups, contradicting solvability). But the simple Abelian groups are cyclic of prime order. Conversely, suppose each N_i/N_{i-1} is cyclic of prime order. Then by the previous problem, G is solvable.

[3B.4] Let H be a complement to N in G (which exists by the Schur-Zassenhaus theorem). Note that $|U|$ and $|N|$ are coprime, so $U \cap N = \{1\}$. Then in the subgroup UN , N is a normal Hall subgroup, so by the Schur-Zassenhaus theorem all complements to N are conjugate in UN (to U). Now let $K = UN \cap H$. We have

$$KN = (UN \cap H)N = UN \cap HN = UN \cap G = UN$$

Since $K \leq H$, we see that $K \cap N = \{1\}$, so $K \leq UN$ is a complement to N in UN . So there's some element $x \in UN$ with $K^x = U$. But then

$$U = K^x \leq H^x$$

and H^x is still a complement to $N^x = N$.

[3B.5] Since $P \leq Z(G)$, we know that $P \triangleleft G$. By the Schur-Zassenhaus theorem, we can write $G = P \rtimes X$ where X is a complement to P . Since P is central however, X acts trivially on P and so we really have $G = P \times X$ is a direct product. Since P is solvable, all complements to P in G are conjugate; but $X \triangleleft G$, so it is the only complement. Since $X \cong G/P$, we see it contains no elements of order divisible by p . Conversely, if $g \in G$ has order not divisible by p , then $|g|$ divides $|G|/|P| = [G : P]$. By the previous problem, $\langle g \rangle$ is contained in some complement to P , namely $g \in X$. So X is precisely the elements of G whose order is not divisible by p .

[3B.6]

- (a) Let $|g| = d$ and let π be the set of primes dividing m . We can write $d = rs$ with r a π -number and r coprime to s . This means we can find integers a, b with $ar + bs = 1$. Now g^r has order s , meaning that $\bar{g}^r \in \bar{G} = G/N$ has order dividing both s and m . But these numbers are coprime, so $\bar{g}^r = 1$. Thus

$$\bar{g} = \bar{g}^{ar+bs} = \bar{g}^{ar} \bar{g}^{bs} = \bar{g}^{bs}$$

and so $N\langle g \rangle = N\langle g^s \rangle$. Choose an integer c with $\bar{g}^{cs} = \bar{g}$. Then g^{cs} is in the coset Ng , and since $g^{csr} = 1$, we see that $|g^{cs}|$ divides r , a π -number. We can thus take $h = g^{cs}$.

- (b) Let $h \in Ng$ be such that $|h| = r$ is a π -number. From $h^m \in N$ we know that $h^{mn} = 1$, where $n := |N|$. Since r and n are coprime, we can find integers a, b with $ar + bn = 1$. Thus

$$h^m = h^{m(ar+bn)} = h^{r(am)} h^{(mn)b} = 1$$

So r divides m . But $\bar{h}$ has order m , and $\bar{h}^r = 1$, so that m divides r . Then $|h| = r = m$, as desired.

- (c) Choose an $x \in G$ with $\bar{g}^x = \bar{g}^{-1}$ and write $H = \langle h \rangle$. Then $\bar{x}$ normalizes $\bar{H} = \langle \bar{g} \rangle$, and so x normalizes HN . Since $|H|$ and $|N|$ are coprime, and H is cyclic (so solvable), all complements to N in HN are conjugate to H . But $H^x \leq HN$, so there is some $hn \in HN$ with

$$H^x = H^{hn} = H^n$$

Thus xn^{-1} normalizes H . But we chose x so that $h^x \in Nh^{-1}$, and we have

$$n(h^x)n^{-1} \in Nh^{-1} \cap H = \{h^{-1}\}$$

and so xn^{-1} conjugates h to h^{-1} .

[3B.7]

- (a) Let $N \triangleleft G = N_r$ be a minimal normal subgroup. Choose the largest $k < r$ such that $N \not\leq N_k$. Then $N \cap N_k = \{1\}$ by minimality, and $N \leq N_{k+1}$ so that N maps isomorphically into N_{k+1}/N_k , a cyclic group. Since N is cyclic, it must be of prime order by minimality (every subgroup of a cyclic group is characteristic).
- (b) Let $M \leq G$ be a maximal subgroup, and let $N \triangleleft G$ be a minimal normal subgroup. We proceed by induction on $|G|$. Now if $N \leq M$, then by induction $[G : M] = [G/N : M/N]$ is prime. If $N \not\leq M$, then since $|N|$ is prime by part (a), we must have $N \cap M = \{1\}$, and $MN = G$ by maximality. Thus $[G : M] = |N|$ is prime in this case as well.

[3B.8]

The conditions of the problem are obvious if G is a p -group, so we assume at least 2 primes divide $|G|$. Let p be the largest prime dividing $|G|$, and q the smallest prime dividing $|G|$; we choose $P, Q \leq G$ to be a Sylow p -subgroup and q -subgroup, respectively. If P is not normal in G , then $N_G(P) \leq M$ for some maximal subgroup M . But $[G : M]$ is prime, and we have by Sylow's theorems

$$1 \equiv [G : N_G(P)] = [G : M][M : N_G(P)] = [G : M][M : N_M(P)] \equiv [G : M] \pmod{p}$$

But no prime dividing $|G|$ can be equivalent to 1 modulo p , since p is the largest prime dividing $|G|$. This contradiction shows we must have P normal in G .

We prove G is solvable by induction on $|G|$. The maximal subgroups of G/P all come from maximal subgroups of G containing P , so that all have prime index. By induction G/P is solvable; but P is solvable, so by Lemma 3.10 we have G is solvable too.

Again, we prove G has a normal q -complement by induction. In G/P there is a normal q -complement K/P , meaning $K \triangleleft G$. By [1B.5] PQ/P is a Sylow q -subgroup of G/P , so that

$$[G : K] = [G/P : K/P] = |PQ/P| = |Q|/|Q \cap P| = |Q|$$

Thus K is a normal q -complement in G .

[3B.9]

We work by induction on $|G|$. Let $N \triangleleft G$ be a minimal normal subgroup, which has prime order p by [3B.7]. If p divides n , then by induction G/N has a subgroup of order n/p , which corresponds to a subgroup of order n in G . If p does not divide n , then G/N has a subgroup of order n by induction, which corresponds to a subgroup $H \leq G$ of order np . But $N \triangleleft H$ is a Hall subgroup, so by the Schur-Zassenhaus theorem there's a complement $K \leq H$, which must have order n .

[3B.10]

This is trivial by part (b) of [3B.7] and [3B.8].

[3B.11] This problem is equivalent to showing no non-trivial Sylow subgroup of G is contained in $\Phi(G)$. Suppose $P \leq G$ is a Sylow p -subgroup contained in $\Phi(G)$. Since $\Phi(G)$ is nilpotent by [1D.14], P is normal (hence characteristic) in $\Phi(G)$, so that $P \triangleleft G$. Then the Schur-Zassenhaus theorem gives a complement $H \leq G$, so that $G = PH$. But $P \leq \Phi(G)$, so that $G = \langle P, H \rangle$ implies $G = H$ (see [1D.7]), and thus $P = \{1\}$.

[3B.12] This problem is incorrect as stated. Let $G = A_4$, with P a Sylow 2-subgroup and Q a Sylow 3-subgroup. Then both P and Q are maximal subgroups of G , so that

$$\Phi(G) \leq P \cap Q = \{1\}$$

Also $P \triangleleft G$, and $G/P \cong Q$, so that G is solvable. But P has a subgroup of index 2, while G does not.

According to math.SE, Isaacs gave an alternative version to the problem: remove the condition that $\Phi(G) = \{1\}$, but add the condition that M be core-free. We handle that case.

Let $N \triangleleft G$ be a minimal normal subgroup of G , and note that $N \not\leq M$ since M is core-free; this means $G = NM$. Now $M \cap N \triangleleft M$, but also $M \cap N \triangleleft N$ since N is Abelian, so $M \cap N \triangleleft NM = G$, and again being core-free implies $M \cap N = \{1\}$. Then for any $H \leq M$, we have

$$[G : NH] = [M : M \cap NH] = [M : (M \cap N)H] = [M : H]$$

Here we have used Dedekind's rule, as well as the fact that $[G : K] = [L : L \cap K]$ when $G = LK$ (here $L = M$ and $K = NH$) [this is Corollary X.11].

[3B.13] Let $X \subset G$ be the subset of normal solvable subgroups, and let $S \in X$ be the largest one by cardinality. We will show every $T \in X$ is contained in S , and hence that S is the unique largest normal solvable subgroup of G .

To that end, note that $ST \triangleleft G$. Also, $T \triangleleft ST$ and we have

$$ST/T \cong S/(S \cap T)$$

Since the right-hand group is a quotient of the solvable group S , it is solvable. Also T is solvable; thus ST is solvable. We have shown $ST \in X$; since $S \leq ST$, maximality implies $S = ST$, so that $T \leq S$, as claimed.

[3B.14] Note that $Z(F) = C \cap F$. Let $S \triangleleft C$ be the unique largest normal solvable subgroup given by the previous problem, so that $Z(F) \leq S$. By [1D.19], we know that $C/Z(F)$ has no non-trivial Abelian normal subgroups. But if $S/Z(F) \neq \{1\}$, the penultimate term of the derived series of $S/Z(F)$ (a solvable group) would be normal in $C/Z(F)$, and it is Abelian. Since this cannot happen, we must have $S = Z(F)$, as desired. Of course, when G itself is solvable, we have $S = C$, so that indeed we have $C = Z(F) \leq F$ in this case.

[3B.15] We prove this by induction on $|G|$. If there is a minimal normal subgroup $N \triangleleft G$ contained in H , then by induction, we have $H/N \triangleleft G/N$, so that $H \triangleleft G$. We show this

case must happen by contradiction. Otherwise, since $H < HN$, we must have $G = HN$. Since $H \cap N \triangleleft H$, and $H \cap N \triangleleft N$ (because N is Abelian), we have $H \cap N \triangleleft G$. But N is minimal normal, so $H \cap N = \{1\}$, and we have $G = NH$, with $[G : H] = |N|$. Let $n \in N$ be a non-trivial element, and let G act on N via conjugation. The orbit of n has size at most $|N| - 1$, and hence

$$[G : C_G(n)] \leq |N| - 1 < |N| = [G : H]$$

and this contradicts the choice of H .

3C

[3C.1] We proceed by induction on $|G|$. Let $N \triangleleft G$ be a minimal normal subgroup of G and $\overline{G} := G/N$; recall that $|N| = p^r$ for some prime p . By induction $\overline{U} \leq \overline{H}$, where $\overline{H}$ is a Hall π -subgroup of $\overline{G}$. This means $U \leq H \leq G$ is such that $[G : H]$ is a π' -number and H/N is a π -group.

Now if $p \in \pi$, then H is a Hall π -subgroup of G , as desired. Otherwise $N \triangleleft H$ is a normal Hall p -subgroup, and $|U|$ divides $[H : N]$. By [3B.4] then, U is contained in a Hall π -subgroup of H , which is also a Hall π -subgroup of G .

[3C.2] Write $K = \bigcap H_p \leq G$. For every $p \in \pi$, a Sylow p -subgroup of K is contained in a Sylow p -subgroup $P \leq G$. But

$$K \cap P \leq H_p \cap P = \{1\}$$

Since this holds for all $p \in \pi$, we see $|K|$ is a π' -number. Now for $q \in \pi'$, and $Q \leq G$ a Sylow q -subgroup, we have $Q \leq H_p$ for all $p \in \pi$, and thus $Q \leq K$. This shows that no $q \in \pi'$ divides $[G : K]$, which must therefore be a π -number. So $K \leq G$ is indeed a Hall π' -subgroup.

[3C.3]

(a) We show that all products of elements of $\mathcal{S}$ are subgroups of G . For that, we proceed by induction on the number of elements. Suppose $(P_1 \cdots P_n) \leq G$ for $P_i \in \mathcal{S}$, and let $Q \in \mathcal{S}$ be another member. Then we have

$$(P_1 \cdots P_n)Q = \{a_1 \cdots a_n q \mid a_i \in P_i, q \in Q\}$$

But

$$a_1 \cdots (a_n q) = a_1 \cdots (a_{n-1} q) \hat{a}_n = \cdots = q \hat{a}_1 \cdots \hat{a}_n$$

where we've repeatedly used that $P_i Q = Q P_i$. This shows $(P_1 \cdots P_n)Q \leq Q(P_1 \cdots P_n)$, and the reverse inclusion is proved the same way, so that $(P_1 \cdots P_n)Q \leq G$. Inductively we've established all these products are subgroups.

From that it's easy to construct a Hall π -subgroup of G . If $\pi = \{p_1, \dots, p_m\}$, then choose $P_i \in \mathcal{S}$ a Sylow p_i -subgroup. Defining $H := P_1 \cdots P_m$ we know from above

that $H \leq G$. Also $[G : H]$ is a π' -number since H contains a Sylow p -subgroup of G for all primes $p \in \pi$. But it's also easy to see inductively that $|H| = \prod |P_i|$, which is a π -number. Thus H is a Hall π -subgroup of G , as desired.

- (b) Since G is solvable, we know it has Hall p' -subgroups H_p for all primes dividing $|G|$; call this set of primes π . Let q be a prime dividing $|G|$, and define K_q to be

$$K_q = \bigcap_{p \in \pi \setminus \{q\}} H_p$$

Then from [3C.2] we know K_q is a Sylow q -subgroup of G . Let $r \in \pi$ be another prime. We show that $K_q K_r \leq G$, which (since q and r were arbitrary) shows that the $\{K_p\}$ are a Sylow system for G . Again by [3C.2], we see that

$$H = \bigcap_{p \in \pi \setminus \{q, r\}} H_p$$

is a Hall $\{q, r\}$ -subgroup of G . By definition $K_q, K_r \leq H$. But then $[H : K_q]$ and $[H : K_r]$ are coprime, so $H = K_q K_r$ is a subgroup, and we're done.

[3C.4] We write $\bar{G} := G/M$. Let $\bar{L} \triangleleft \bar{G}$ be a minimal normal subgroup, which must be an elementary Abelian q -group for some prime q . Now M is also an elementary Abelian p -group for some prime p . If $p = q$, then $L \triangleleft G$ is a normal p -subgroup of G . Since $Z(L) \triangleleft G$ and $Z(L) \cap M > \{1\}$ (because we're in a p -group), minimality implies $M \leq Z(L)$, so that $M < L \leq C_G(M)$, and that contradicts our hypotheses. Thus we must have $p \neq q$.

Let $Q \leq L$ be a Sylow q -subgroup of $L \triangleleft G$, so that $L = QM$. By Frattini's argument, we have $G = N_G(Q)L = N_G(Q)M$. Since $N_G(Q) \cap M$ is normal in both $N_G(Q)$ and M , minimality implies either $M \leq N_G(Q)$ (so $Q \triangleleft G$) or $N_G(Q) \cap M = \{1\}$. The first case can't happen since then $Q \leq C_G(M)$, so we must be in the second case, and $N_G(Q)$ is a complement to M in G .

Finally let $C \leq G$ be another complement to M in G . Then $[G : C] = |M|$ implies C contains some conjugate of Q , say $Q^g \leq C$. By conjugating everything by g^{-1} , we may as well assume $Q \leq C$. The quotient map $G \rightarrow G/M$ induces an isomorphism $C \rightarrow \bar{C}$; since Q maps to $\bar{L} \triangleleft \bar{G}$, this isomorphism shows $Q \triangleleft C$. In other words, $C \leq N_G(Q)$, and order considerations then show $C = N_G(Q)$.

[3C.5] Let $M \triangleleft G$ be a minimal normal subgroup, and note since H is core-free we must have $M \not\leq H$; maximality then implies $G = MH$. Now $H \cap M$ is normal in both H and M , so by minimality $H \cap M = \{1\}$; thus H complements M . Because $C_G(M) \triangleleft G$, we have $C_H(M) = H \cap C_G(M)$ is normal in H . But it also centralizes M , so it is normalized by M , and thus $C_H(M) \triangleleft MH = G$. Since H is core-free, we see that $C_H(M) = \{1\}$. Dedekind's rule then shows

$$C_G(M) = MH \cap C_G(M) = M(H \cap C_G(M)) = MC_H(M) = M$$

If $N \triangleleft G$ was any other minimal normal subgroup of G , then $M \cap N = \{1\}$ would imply $N \leq C_G(M)$, and from the above that means $N \leq M$. In other words, M is the unique minimal normal subgroup of G . If $K \leq G$ is also maximal with trivial core, then the argument above shows K complements M in G . The previous problem then shows H and K are conjugate.

[3C.6] We work by induction on the derived length of G , the case of derived length 0 being trivial. Let $N \triangleleft G$ be the penultimate term of the derived series, so that N is Abelian. The inductive hypothesis (applied to G/N) shows $x, y, z \in N$. Suppose x has order a , y order b , and z order c . If $a > 1$, then let $k = (a + 1)bc$, which is not divisible by a (here we use the pairwise relatively prime orders hypothesis). Then

$$1 = (xyz)^k = x^k y^k z^k = x^k \neq 1$$

and this contradiction shows we must have $a = 1$ and $x = 1$. The same argument shows $y = z = 1$ as well.

[3C.7]

(a) We work by induction on $|G|$. Let $N \triangleleft G$ be a minimal normal subgroup, and define $\bar{G} := G/N$. Then by induction there is a Carter subgroup $\bar{K} \triangleleft \bar{G}$, coming from a subgroup $N \leq K \leq G$. In particular, note that $N_G(K) = K$.

First we construct a complement in K : let $P \leq K$ be a Sylow p -subgroup, where N is an elementary Abelian p -subgroup. Then $\bar{P} \triangleleft \bar{K}$ by nilpotence, so $P \triangleleft K$. Define U to be a complement to P in K , which exists by the Schur-Zassenhaus theorem. Because $U \cong \bar{U} \leq \bar{K}$, U is nilpotent.

Now we "grow" U until it becomes like a complement to N in K . Define $C = N_K(U)$. By Dedekind's rule we have

$$N_K(U) = N_K(U) \cap PU = (N_K(U) \cap P)U$$

If $x \in P$ normalizes U , then for all $u \in U$ we have $[x, u] \in U \cap P = \{1\}$; this shows $N_K(U) \cap P = C_P(U)$ so that $C = UC_P(U)$. Because C is the internal direct product of two nilpotent groups, it is nilpotent. Let $x \in P$; because $\bar{U} \triangleleft \bar{K}$, we know that $NU \triangleleft K$. Thus $U^x \leq NU$, and by Schur-Zassenhaus applied to NU , we see that U^x is conjugate to U , so there's an $n \in N$ with $U^{x^n} = U$. This shows $x \in N_K(U)N$, and since $x \in P$ was arbitrary we have

$$K = UP \leq N_K(U)N = CN$$

Finally we show C is self-normalizing in G , so it is a Carter subgroup. Now if $g \in G$ normalizes C , then

$$K^g = (CN)^g = C^g N^g = CN = K$$

so that $g \in N_G(K) = K$. So it's enough to show that $N_K(C) = C$. But U is characteristic in C , so anything normalizing C also normalizes U . This shows $N_K(C) \leq N_K(U) = C$, as desired.

- (b) Let $H, K \leq G$ be Carter subgroups of G . We use induction on $|G|$ to work towards the case that H and K are maximal core-free subgroups of G , and then apply [3C.5]. First we establish that for any non-trivial normal subgroup $N \triangleleft G$, with $\overline{G} := G/N$, then $\overline{H}$ and $\overline{K}$ are Carter subgroups, so that by induction they're conjugate (meaning HN and KN are conjugate). Obviously $\overline{H}$ and $\overline{K}$ are nilpotent, so it's enough to show $N_G(HN) = HN$ (the KN case follows similarly). This is obvious if $HN = G$, so assume $HN < G$. If $(HN)^g = HN$, then $H, H^g \leq HN$ are Carter subgroups, and by induction there's $n \in N$ with $H^{g^n} = H$. Thus $g \in N_G(H)N = HN$, as desired.

Now if $N \triangleleft G$ is a minimal normal subgroup, then from the above there's $g \in G$ with $(HN)^g = KN$. Replacing H with H^g , we can assume $HN = KN$. If $HN < G$ then the inductive hypothesis again shows H is conjugate to K (in HN), so we have reduced to the case $G = HN = KN$. If $M \triangleleft G$ is a minimal normal subgroup of G contained in H , then from above $HM = H$ is conjugate to KM , and K is contained in some conjugate H^x of H . Since H^x is nilpotent and normalizers grow in nilpotent groups, K being self-normalizing implies $K = H^x$, and we're done. So we've reduced to the case where H is core-free (and similarly K is core-free).

Finally we note that if $H \leq M \leq G$, then Dedekind's rule says

$$M = M \cap NH = (M \cap N)H$$

Since $M \cap N$ is normal in both M and N , minimality of N implies $M \cap N = \{1\}$ (so $M = H$), or $M \cap N = N$ (so $M = G$). Thus H (and similarly K) is a maximal subgroup of G . Now appeal to [3C.5] shows H and K are conjugate.

- (c) Let $N \triangleleft G$ and $C \leq G$ a Carter subgroup. If $g \in N_G(CN)$, then we have $C^g \leq CN$ is a Carter subgroup of CN . By part (b) above, we then know there is an $n \in N$ with $C^n = C^g$, so that $gn^{-1} \in N_G(C) = C$, and hence $g \in CN$. This shows $N_G(CN) = CN$.

If now $\overline{G} := G/N$ is nilpotent, then we've just seen that $\overline{C} = \overline{CN}$ is self-normalizing. But normalizers grow in nilpotent groups, so $\overline{C} = \overline{G}$, and hence $G = CN$.

[3C.8] Let $H, K \leq G$ be nilpotent injectors. We will show H and K are conjugate by conjugating one Sylow subgroup at a time.

Let π be the primes dividing $|G|$, and for $p \in \pi$ we define $H_p \leq H$ to be the Sylow p -subgroup of H (unique because H is nilpotent). Write $C_p \leq F(G)$ to be the (normal) p -complement in $F(G)$. Then because H is nilpotent, H_p centralizes C_p , and $H_p \leq C_G(C_p)$. Choose a Sylow p -subgroup $S_p \leq C_G(C_p)$ containing H_p . Since $C_G(C_p) \triangleleft G$, we see that for $p \neq q$

$$[C_G(C_p), C_G(C_q)] \leq C_G(C_p) \cap C_G(C_q) \leq C_G(F(G)) \leq F(G)$$

where the last containment follows from [3B.14]. This shows $C_G(C_p)$ normalizes $S_q F(G) \leq C_G(C_q) F(G)$, but we have $O_q(G) \leq S_q$ so that $S_q F(G) = S_q C_q$ is a direct product (since S_q centralizes C_q). Thus S_q is normal (hence characteristic) in $S_q F(G)$, and thus $C_G(C_p)$ normalizes S_q . Note this works with any Sylow q -subgroup of $C_G(C_q)$.

3D

In particular, S_p normalizes S_q , and this works for all primes $p, q \in \pi$. We can thus form the subgroup $I = \prod S_p$, which is nilpotent (all Sylow subgroups are normal), and also contains $F(G)$ (since $O_p(G) \leq S_p$ for all $p \in \pi$). By construction, I contains every Sylow of H , and hence contains H . Maximality then implies $H = I$. If we do the same procedure for K , we can write it as $K = \prod T_p$, where $T_p \leq C_G(C_p)$ is a Sylow p -subgroup for all primes $p \in \pi$. But S_p and T_p are conjugate in $C_G(C_p)$, say by an element $x_p \in C_G(C_p)$. As shown above, x_p normalizes S_q (and all Sylow q -subgroups of $C_G(C_q)$) for all $p \neq q$, hence

$$H^{x_p} = T_p \prod_{q \neq p} S_q$$

Finding an element $x_p \in C_G(C_p)$ for all $p \in \pi$, and defining $x := \prod x_p$, we then see that $H^x = \prod T_p = K$, and thus H and K are conjugate.

3D

[3D.1]

- (a) By the Hall-Higman theorem, we see that $C_G(O_p(G)) \leq O_p(G)$. But $O_p(G) \leq P$, so that $Z(P) \leq C_G(O_p(G))$, and we're done.
- (b) We can prove this by induction on $|G|$. If $O_{p'}(G) > 1$, then the inductive hypothesis applies to $\bar{G} := G/O_{p'}(G)$, which must then have p -length at most the nilpotence class of $\bar{P} \cong P$. Since the p -length of $\bar{G}$ is the p -length of G , we have reduced to the case $O_{p'}(G) = \{1\}$.

In that case, part (a) shows $Z(P) \leq O_p(G)$; let the nilpotence class of P be c . By induction, the p -length of $\bar{G} := G/O_p(G)$ is at most the nilpotence class of $\bar{P}$, which (being a quotient of $P/Z(P)$) is at most $c - 1$. Since the p -length of $\bar{G}$ is one less than that of G , we see that the p -length of G is at most $(c - 1) + 1 = c$, and we're done.

[3D.2]

Let $K = O_\pi(G)$ and write $\bar{G} := G/Z$. Since $\bar{K} \triangleleft \bar{G}$ is a π -group, we see that $K \leq O_\pi(\bar{G})$. Let $L \triangleleft G$ be the subgroup containing Z such that $\bar{L} = O_\pi(\bar{G})$. We will be done if we can show $L \leq KZ$. If $C \leq Z$ is the (normal) Hall π' -subgroup, then $C \triangleleft L$, and $[L : C] = [L : Z][Z : C]$ is a π -number. The Schur-Zassenhaus theorem then shows we have a complement $H \leq L$ with $L = CH$. Since $C \leq Z$ is central, we see that H is a normal Hall π -subgroup of L , and hence $H \triangleleft G$. This means that $H \leq K$, so we have $L = HC \leq KZ$, as desired.

[3D.3]

Let $\bar{G} := G/Z(G)$. From the previous problem we see that

$$O_\pi(\bar{G}) = \overline{O_\pi(G)} = \{1\}$$

since $O_\pi(G) \leq Z(G)$. Similarly, $O_{\pi'}(\bar{G}) = \{1\}$. Since $\bar{G}$ is π -separable, this is only possible if $\bar{G} = \{1\}$, so that $G = Z(G)$ is Abelian.

[3D.4] Let $P \leq H$ be a Sylow p -subgroup of H . Because P fixes every coset of $\Phi(G)$, and since each coset has $|\Phi(G)| \not\equiv 0 \pmod{p}$ elements, it must be that the set of fixed points of P on this coset is non-empty. Let $\{x_1, \dots, x_n\}$ be coset representatives for $\Phi(G) \leq G$, with $[G : \Phi(G)] = n$, and such that P fixes each x_i . Then the x_i are contained in $C_G(P)$, and hence

$$G = \langle x_1, \dots, x_n \rangle \Phi(G) = \langle x_1, \dots, x_n \rangle$$

shows that $G = C_G(P)$, so that P acts trivially on G . Since this works for any Sylow subgroup of H , and H is generated by its Sylow subgroups, we see that H acts trivially on G .

[3D.5] First suppose $O_{p'}(G) = \{1\}$. Now if K is a p' -subgroup, such that $P \leq N_G(K)$, then

$$[O_p(G), K] \leq O_p(G) \cap K = \{1\}$$

so that $K \leq C_G(O_p(G)) \leq O_p(G)$ by the Hall-Higman theorem. But then K is also a p -group, so that $K = \{1\} \leq O_{p'}(G)$, as desired.

More generally, let $\bar{G} := G/O_{p'}(G)$, so that $O_{p'}(\bar{G}) = \{1\}$. Since $\bar{P}$ is still a Sylow p -subgroup of $\bar{G}$, the previous paragraph shows $\bar{K} = \{1\}$, so that $K \leq O_{p'}(G)$, and we're done.

3E

[3E.1] We assume throughout that G and A are non-trivial. First assume that G is solvable. Then G has a characteristic non-trivial Abelian subgroup $N \leq G$ (this is just the last non-trivial term of the derived series for G). Choose p a prime dividing $|N|$. Then the Sylow p -subgroup $P \leq N$ is characteristic in G , and thus fixed by all automorphisms, including those in A . So P is our A -invariant subgroup.

So now we can assume that A is solvable, so has a minimal normal subgroup $P \triangleleft A$ that is a p -group for some prime p . First suppose that $C_G(P) = \{1\}$. Then since

$$|G| \equiv |C_G(P)| \pmod{p}$$

we see that p does not divide $|G|$. Pick any prime q dividing $|G|$, and let $Q \leq G$ be a P -invariant Sylow q -subgroup, guaranteed by Theorem 3.23. Now if $\hat{Q}$ was another P -invariant Sylow q -subgroup, then Theorem 3.23 would again imply that Q and $\hat{Q}$ are conjugate via an element of $C_G(P) = \{1\}$, and so $\hat{Q} = Q$. Thus there is a unique P -invariant Sylow q -subgroup of G . If $a \in A$, then Q^a is also P -invariant (since P is normal in G), so uniqueness implies $Q^a = Q$. Thus $Q \leq G$ is our A -invariant q -subgroup.

If $C_G(P) > 1$, then for all $x \in C_G(P)$, we have $x^a \in C_G(P)$ (since P is normal in A), hence $C_G(P)$ is A -invariant, acted on by A/P . We can thus replace G with $C_G(P)$ and A with A/P and repeat the above reasoning. Either we end up in a case where $C_G(P) = \{1\}$ (so

we're done by the previous paragraph), or we reduce to the case $A = \{1\}$, in which case any p -subgroup of G will do.

[3E.2] Let $C = C_G(A)$ and since $G = HK$, we can write $c = hk$. Then via Theorem 3.27 we know that the coset hK is A -invariant. This means that for every $a \in A$, we have $h^a \in hK$, and thus $h^{-1}h^a \in H \cap K$. Put another way, $h^a \in h(H \cap K)$ for all $a \in A$. Since $H \cap K$ is A -invariant, this shows $h(H \cap K)$ is an A -invariant coset, so applying Theorem 3.27 again we find that there is $x \in H \cap K$ with $hx \in C \cap H$. But then

$$x^{-1}k = (hx)^{-1}(hk) \in C \cap K$$

and so $c = hk = (hx)(x^{-1}k) \in (C \cap H)(C \cap K)$. Because $c \in C$ was arbitrary, we have shown $C = (C \cap H)(C \cap K)$.

[3E.3] Let $a \in A$ and write $B = \langle a \rangle$. It is enough to show B acts trivially on G . By Corollary 3.28, we have (with $\overline{G} := G/N$)

$$\overline{G} = C_{\overline{G}}(B) = \overline{C_G(B)}$$

where the first equality follows because A (and hence B) acts trivially on $\overline{G}$ by hypothesis. Thus $G = C_G(B)N$. But $N \leq C_G(A) \leq C_G(B)$ by hypothesis as well, so $G = C_G(B)$ and B acts trivially on G , as desired.

[3E.4] Since $|HC| = |H| \cdot |C| / |H \cap C|$, this problem is equivalent to showing $|HC|$ divides $|G|$. Let p be any prime, and let $|X|_p$ denote the highest power of p dividing $|X|$; when X is a group, then $|X|_p$ is just the order of a Sylow p -subgroup. Then showing $|HC|$ divides $|G|$ is equivalent to showing $|HC|_p \leq |G|_p$ for all primes p . And finally, this is implied by showing that there's a Sylow p -subgroup P of G containing both a Sylow p -subgroup Q of H and a Sylow p -subgroup R of C . To see this, note that it implies

$$|HC|_p = \frac{|H|_p \cdot |C|_p}{|H \cap C|_p} \leq \frac{|Q| \cdot |R|}{|Q \cap R|} = |QR| \leq |P| = |G|_p$$

To find such a P , let $Q \leq H$ be an A -invariant Sylow p -subgroup, given by Theorem 3.23. Now choose an A -invariant Sylow p -subgroup $P \leq G$ containing Q using Corollary 3.25. Then we can take $R = P \cap C$ by Lemma 3.32, and we're done.

[3E.5] Obviously P acts trivially on P/F . Because both P and F are normal in G , we see that the kernel K of this action is a normal subgroup of G . If $k \in K$ has order coprime to p , then from Corollary 3.29, we see that

$$k \in C_G(P) \leq P$$

where the final containment follows from the Hall-Higman theorem. Since $|k|$ is coprime to p we see $k = 1$. Thus K is a p -group of G , and by normality we must have $K \leq P$, and hence $K = P$, as desired.

3F

[3F.1] We have $C \triangleleft G$ of index 2, so of course G/C is a cyclic extension. Also since every element of order 2 is contained in C , which is cyclic, we see G has exactly one element $z \in G$ of order 2, which must be central. Let $g \in G \setminus C$. Then since $|g| = 4$ we must have $g^2 = z$. If $c \in C$, then since $gc \notin C$ we have

$$(gc)^2 = z$$

Since $z = g^2$, this can be rewritten to $c^g = c^{-1}$. Thus gC generates G/C ; $g^2 = z \in C$ and $z^g = z$; and $c^g = c^{-1}$. By Theorem 3.35 applied to $C \triangleleft G$ and the cyclic subgroup N of index 2 in Q_n (using the identity isomorphism between C and N), we see G is isomorphic to Q_n .

[3F.2] We prove this by induction on $|G|$. By [3B.3], we know that G has a normal subgroup $N \triangleleft G$ of prime index. Thus G/N is cyclic, and we can choose $g \in G$ such that gN generates G/N . Let us write $m = |G/N|$, $\sigma \in \text{Aut}(N)$ for conjugation by g , and $\alpha \in N$ as g^m . Theorem 3.36 then shows how to construct G from N . Since (by induction) we can use Theorem 3.36 repeatedly to construct N from the trivial group, we see we can do the same for G .

[3F.3] Let $C \triangleleft Q$ be the cyclic group of index 2 used to construct Q . Since $|Q \setminus C| = 4$ and it consists solely of elements of order 4, we can pair them up (via inversion) to produce 2 more cyclic subgroups of order 4, which we call A and B .

Let $c \in C$ be an element of order 4. Then $c^2 \in A \cap B$ is the unique element of order 2, and as shown in [3F.1] c acts by inversion on A and B . Pick $N = A$ and $N_0 = B$, with $G = G_0 = Q$. Then cN generates G/N and cN_0 generates G/N_0 . Since c acts by inversion on both A and B , Theorem 3.35 shows there is an isomorphism between G and G_0 , sending A to B . This gives an automorphism of Q sending A to B . Any permutation of $\{A, B, C\}$ gives an automorphism as above sending one cyclic subgroup to the other; thus $\text{Aut}(Q)$ acts transitively on $\{A, B, C\}$.

[3F.4] Let $S := SL(2, 3)$ act on the two-dimensional vector space V over $\mathbb{F}_3$. Then S acts transitively on the 8 points V^* , and the elements fixing the vector $(1, 0)$ are exactly those that are upper triangular with 1s on the diagonal, of which there are $3 = |\mathbb{F}_3|$. Hence $|S| = 24$. We write $I \in S$ for the identity matrix. We can figure out possible element orders in S by looking at minimal polynomials $m(t)$ for some $X \in S$. To do this, we note that $\deg(m) \in \{1, 2\}$ and that when $m(t)$ has degree $2 = \dim(V)$, its constant term must be equal to $\det(X) = 1$. This gives the possibilities:

- If $m(t) = t - 1$, then $X = I$ is the identity.
- If $m(t) = t + 1$, then $X = -I$.
- If $m(t) = t^2 + 1$, then $X^2 = -I$ so $|X| = 4$.
- If $m(t) = t^2 + t + 1 = (t - 1)^2$, then since $t^3 - 1 = (t - 1)^3$, we see that $X^3 = I$.

- If $m(t) = t^2 - t + 1 = (t + 1)^2$, then since $t^3 + 1 = (t + 1)^3$, we see that $X^3 = -I$ so that $|X| = 6$.

So we see that S has a unique element $-I$ of order 2, and that every element has order in the set $\{1, 2, 3, 4, 6\}$. If $Z = \{\pm I\}$, then $Z \leq Z(S)$. Let $Q \leq S$ be a Sylow 2-subgroup. Then $|Q| = 8$ and from the above, $Q \setminus Z$ is all elements of order 4. It thus has a cyclic subgroup $C \leq Q$ of order 4, with all elements of $Q \setminus C$ also of order 4. By [3F.1] we see $Q \cong Q_8$.

Let $P \leq S$ be a Sylow 3-subgroup, and assume $P \triangleleft S$. Then the normalizer-centralizer theorem implies $|C_S(P)| \geq 12$, and thus there's an element of order 4 centralizing a generator for P , giving an element of order 12 in S . From the above list, that's impossible, so P is not normal in S .

Since $Z(S) \neq \{1\}$, we know that $S \not\cong S_4$. Thus by Theorem 1.33, we see that Q is normal in S , and we're done.

[3F.5] $G := GL(2, 3)$ has order $(3^2 - 1)(3^2 - 2) = 48$, since this is the number of ways to choose an ordered basis of $\mathbb{F}_3^2$; thus $[G : S] = 2$. We also have

$$g = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in G \setminus S$$

has order 2. But for every $X \in G$, we have $X^2 \in S$. If $|X| = 4$ then $X^2 = -I$ by the previous problem. This means that X satisfies the polynomial $t^2 + 1 = 0$, implying that $\det(X) = 1$, so $X \in S$. Thus $G \setminus S$ has no elements of order 4. It's possible to list an explicit element of order 8 in $G \setminus S$:

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^4 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

The matrix above comes from the factorization (over $\mathbb{F}_3$) of $t^4 + 1 = (t^2 - t - 1)(t^2 + t - 1)$; it is the rational canonical form corresponding to the first quadratic.

Let $\sigma \in \text{Aut}(S)$ be the automorphism induced via conjugation by g . Note that $|\sigma| = 2$ and $\sigma(-I) = -I$; because $-I \in Z(S)$ Theorem 3.36 allows us to construct a group H with $S \triangleleft H$ of index 2, with an element $h \in H$ acting on S as σ . We have $h^2 = -I$ so that $|h| = 4$. Suppose now that hs had order 2; then we would have

$$I = (hs)^2 = h^2 s^h s = -s^h s = -s^8 s = -(gs)^2$$

implying that $(gs)^2 = -I$ so that $|gs| = 4$. But as shown above, no element of $G \setminus S$ has order 4, so hs cannot have order 2. Finally, let $s \in S$ be such that $|gs| = 8$, which exists as shown above. Then

$$-I = (gs)^4 = (s^8 s)^2 = (s^h s)^2 = (-(hs)^2)^2 = (hs)^4$$

where the last two equalities follow from $h^{-2} = -I$ and $-I \in Z(S)$. Thus we have $|hs| = 8$ and $hs \in H \setminus S$.

4A

[4A.1] Note that $[A, B] \triangleleft \langle A, B \rangle = G$ by Lemma 4.1. But then $\bar{A}$ and $\bar{B}$ centralize each other in $\bar{G} := G/[A, B]$ by Lemma 4.2, and since they're both Abelian, we see that $\bar{G}$ is Abelian, and hence $G' \leq [A, B]$. Since the other containment is obvious, we have shown that $G' = [A, B]$.

[4A.2] Obviously the only way for $[h, k, l]$ to be non-trivial is if all of $\{h, k, l\}$ are non-trivial, and that can only happen in one way when H, K , and L all have order 2. Now let $G = A_5$ and let $P \leq G$ be a Sylow 5-subgroup. Since G is simple, Sylow theory shows $[G : N_G(P)] = n_5(G) = 6$, so that $N_G(P)$ has order 10. Let $H \leq N_G(P)$ be a Sylow 2-subgroup. If H was normal in $N_G(P)$, then $N_G(H)$ would contain a Sylow 2-subgroup and Sylow 5-subgroup of G , implying $[G : N_G(H)] \leq 3$, which contradicts the simplicity of G (via the $n!$ theorem). So $N_G(P)$ has more than one Sylow 2-subgroup; let $K \neq H$ be another one. Then

$$H < \langle H, K \rangle \leq N_G(P)$$

implies $N_G(P) = \langle H, K \rangle$. Now H cannot normalize K and $[H, K] \triangleleft N_G(P)$, so we must have $P \leq [H, K]$. Let $L \leq G$ be subgroup of order 2 which doesn't normalize P ; this exists since $N_G(P)$ doesn't have any subgroup of order 4, so for example we can choose L such that HL is a Sylow 2-subgroup of G . Then $R := \langle P, L \rangle$ has order larger than 10, so $[G : R] \leq 3$, and again by the $n!$ theorem we have that $R = G$. But $[H, K, L]$ must be non-trivial, since L does not centralize $P \leq [H, K]$. Meanwhile

$$[H, K, L] \triangleleft \langle [H, K], L \rangle \geq \langle P, L \rangle = G$$

implies (by simplicity) that $G = [H, K, L]$.

[4A.3] Choose $A \triangleleft G$ and $B \leq G$ such that $\bar{G} = \bar{A} \bar{B}$ is a quasiquaternion decomposition for $\bar{G} := G/Z$. Since $Z \leq Z(G)$, we see that – since their images in the quotient are cyclic – A and B must be Abelian. So we have $G = AB$ and of course $A \cap B \leq Z(G)$. Note $G/A \cong B/(A \cap B)$ is a quotient of $\bar{B}$, hence cyclic. Let $b \in B$ be the preimage of a generator of $\bar{B}$, and note that Lemma 4.6 shows the map $A \rightarrow G'$, given by $a \mapsto [a, b]$, is a surjective homomorphism, with kernel $A \cap Z(G)$.

Assume $Z > 1$, and we reach a contradiction. Choose $a \in A$ with $1 \neq [a, b] \in Z$. Note that this means $a \notin Z(G)$, so $a \notin B$. In G/Z then, we see

$$\bar{a} \notin \overline{A \cap B} = \bar{A} \cap \bar{B} = Z(\bar{G})$$

But $\bar{a}$ is centralized by $\bar{A}$, and we know that $[\bar{a}, \bar{b}] = \overline{[a, b]} = 1$, so that the cyclic group $\bar{B}$ also centralizes $\bar{a}$. In particular, we have $\bar{a} \in Z(\bar{G})$, and that is our contradiction. So we must have $Z = \{1\}$.

[4A.4] Since $P/Z(P)$ is Abelian, P has nilpotence class 2. Since P' is elementary Abelian, Lemma 4.4 shows $P/Z(P)$ is elementary Abelian as well.

[4A.5]

- (a) If $z \in P$, then $x^z = x[x, z] \in xP'$, so the conjugacy class of x is contained in the coset xP' , of size $|P'| = p$. Since x is assumed non-central, its conjugacy class must then have size p , implying $[P : C_P(x)] = p$.
- (b) Since $[x, y] \neq 1$ by hypothesis, it must generate $P' = Z(P)$, so that $Z(P) \leq U$. But $\bar{P} := P/Z(P)$ is elementary Abelian by the previous problem, hence so is $U/Z(P)$. This means $\bar{x}$ and $\bar{y}$ each have order p in $\bar{U}$ (since neither is central), and we cannot have $|\bar{U}| = p$, because that would force U to be Abelian. So $|\bar{U}| = p^2$, implying

$$|U| = |\bar{U}| \cdot |Z(P)| = p^3$$

- (c) Note that $V = C_P(x) \cap C_P(y)$, which has index at most p^2 by (a). If the index is p , then $C_P(x) = C_P(y)$, implying $x \in C_P(x)$ centralizes y , contradicting our hypothesis. Thus $[P : V] = p^2$.
- (d) First note a few things. $Z(G) \leq C_P(U) = V$, so $Z(G) \leq Z(V)$. Also since $|U| = p^3$ and U is non-Abelian, we must have $|Z(U)| = p$ (and in fact U is extraspecial). As shown in the previous part, $Z(G) \leq U$, so we have $Z(U) = Z(G)$. Finally, $V \cap U = Z(U) = Z(G)$. But then

$$|UV| = \frac{|P| \cdot |U|}{p^2 \cdot |Z(G)|} = |P|$$

and hence $P = UV$. Because $Z(V)$ is centralized by V and by U (since $V = C_P(U)$), it must be that $Z(V) \leq Z(G)$, and we have equality. Then $Z(V)$ has order p , and $V/Z(V) \leq P/Z(G)$ is Abelian, so that $V' \leq Z(V)$. However V is not Abelian: $P > U$ implies $|P| > p^3$, so that $|V| > p$, and thus $V > Z(V)$. So we indeed have $V' = Z(V)$ of order p , and V is extraspecial.

- (e) Assume by induction that all extraspecial groups of order less than $|P|$ have center with index p^{2r} for some positive integer r . If $P = U$, then $|P| = p^3$ and $|Z(P)| = p$ implies $[P : Z(P)] = p^2$. So we can assume $P > U$, and thus by part (d) we have that V is extra-special. Then by parts (b) and (d) we have

$$[P : Z(P)] = [P : V][V : Z(V)] = p^2[V : Z(V)] = p^{2+2r}$$

with the last equality following from the inductive hypothesis. Then $[P : Z(P)] = p^{2e}$ with $e = r + 1$.

[4A.6] Focusing on the non-trivial N case, choose a minimal k such that $\gamma^k(P) < N$. Then in $\bar{P} := P/\gamma^k(P)$, we have $\bar{N} \cap Z(\bar{P}) > 1$. The hypothesis $[P : N] \geq p^2$ implies $k > 2$, and the fact P is maximal class then implies that $Z(\bar{P})$ has order p , and

$$Z(\bar{P}) = \gamma^{k-1}(\bar{P}) = \overline{\gamma^{k-1}(P)}$$

Thus $Z(\bar{P}) \leq \bar{N}$, meaning that $\gamma^{k-1}(P) \leq N$. Minimality of k then implies $N = \gamma^{k-1}(P)$. Since this argument depends only on $|N|$, we see that N is the unique normal subgroup of its order in P .

[4A.7] Let $P = A \rtimes U$, and note that $[P : A] = |U| = p$, so that for every $x \in P$, $x^p \in A$. Since every element in A has order dividing p^n , we see that every element in P has order dividing p^{n+1} . So we are done if we can find an element of order exactly p^{n+1} . Let $c \in C$ be a generator, and write $f \in A$ as

$$f(m) = \begin{cases} c & m = 1 \\ 1 & m \neq 1 \end{cases}$$

If we let $g := uf$, then we have

$$g^2 = u^2 f^u f$$

Note that $f^u(m)f(m) = c$ precisely when $m \in \{1, 2\}$. Similar reasoning and induction show that, for $1 \leq k \leq p$, we have $g^k = u^k f_k$, where $f_k(m) = c$ precisely when $m \leq k$. Then $g^p = f_p$ is a constant function of order $|c| = p^n$, implying $|g| = p^{n+1}$.

[4A.8]

- (a) If $au^x \in Z(P)$ then u^x centralizes A , so $x = 0$. Thus $Z(P) \leq A$, and $Z(P) = C_A(U)$. Since conjugation by u cycles the coordinates of an element of A , being in $C_A(U)$ means all coordinates are equal, so that $Z(P)$ is exactly the set of constant functions in A . Note that $|Z(P)| = |C| = p^n$.
- (b) By [4A.1] we see that $P' = [A, U]$; since $A \triangleleft P$ we have $[A, U] \leq A$. Because $P/A \cong U$ is cyclic, Lemma 4.6 actually shows all elements of $[A, U]$ look like $[a, u]$ for $a \in A$. And we have

$$[a, u](m) = a^{-1}(m)a^u(m) = a^{-1}(m)a(m-1)$$

where our arithmetic is happening modulo p . This is enough to show

$$\prod_{m=1}^p [a, u](m) = \prod_{m=1}^p a^{-1}(m)a(m-1) = a(p)a^{-1}(1)a(1)a^{-1}(2)a(2) \cdots a(p) = 1$$

Thus $P' \leq K = \{f \in A \mid \prod f(m) = 1\}$. Conversely, if $f \in K$, then define

$$g(m) = \prod_{k=1}^m f^{-1}(k)$$

It's easy to see from the above formulas that $[g, u](m) = f(m)$. Note that we need $f \in K$ because $g(1) = f^{-1}(1)$ while $[g, u](1) = f(1)g(p)$, so we need $g(p) = 1$. We've shown $K = P'$, as desired.

- (c) We have $Z(P'U) = Z(P) \cap P'$ by (a) and the fact $P' \leq A$ is Abelian. By the previous parts we see that $Z(P) \cap P'$ is exactly the set of constant functions $f(m) = x$, with $x^p = 1$. There are p such $x \in C$, so $Z(P'U)$ has order p .
- (d) P/A is cyclic, and $A \cap Z(P) = Z(P)$ has order p^n by part (a). So if $n = 1$, Theorem 4.7 shows P has class p , while $|P| = p^{p+1}$, so P is maximal class. Part (b) shows $|P'| = p^{n(p-1)}$, and part (c) with Theorem 4.7 shows $P'U$ has class $n(p-1)$, so $P'U$ also is maximal class (since $|P'U| = p|P'|$).

[4A.9]

- (a) First suppose $A \triangleleft \triangleleft G$. Then we have a normal series $A = K_r \triangleleft K_{r-1} \triangleleft \cdots \triangleleft K_1 \triangleleft G$. Because $K_1 \triangleleft G$, we know that

$$K_1 \geq [M, K_1] \geq [M, A] = M$$

Then repeatedly applying the same reasoning shows $M \leq K_i$ for $i \geq 1$, so that eventually $M \leq A$.

Conversely, suppose $M \leq A$, and define $N_1 = N$, $N_2 = [N, A]$, etc. We let $N_r = M$ be the last term. Consider now the subgroups $K_i := N_i A$, with $K_r = A$. Since $N_{i+1} = [N_i, A]$, Lemma 4.1 implies N_{i+1} is normal in K_i . Also, since A normalizes A we have $K_{i+1} \triangleleft K_i$. But $K_1 = NA = G$, so the K_i give a subnormal series for $A \leq G$.

- (b) We prove by induction on n that $M \leq \gamma^n(A)$ for all positive integers n . The base case $n = 1$ is by hypothesis. Assuming $M \leq \gamma^n(A)$, then we have

$$M = [M, A] \leq [\gamma^n(A), A] = \gamma^{n+1}(A)$$

Thus $M \leq A^\infty$.

[4A.10]

We proceed by induction on n , the base case $n = 0$ being when P is Abelian, so $P' = 1$. Now if P is non-Abelian, we choose a maximal subgroup $Q \triangleleft P$ containing the proper subgroup $Z(P)$. Since then

$$[Q : Z(Q)] \leq [Q : Z(P)] = p^{n-1}$$

the inductive hypothesis shows $|Q'| \leq p^{(n-1)(n-2)/2}$. We now work in the quotient $\bar{P} := P/Q'$, which has a maximal Abelian subgroup $\bar{Q} \triangleleft \bar{P}$. Now $\overline{Z(P)} \leq Z(\bar{P})$, so we have

$$[\bar{Q} : \bar{Q} \cap Z(\bar{P})] \leq [\bar{Q} : \bar{Q} \cap \overline{Z(P)}] = [\bar{Q} : \overline{Z(P)}] = [Q : Z(P)Q'] \leq [Q : Z(P)] = p^{n-1}$$

Lemma 4.6 then shows that $[\overline{P, P}] = [\bar{P}, \bar{P}]$ has order at most p^{n-1} . We have thus shown what we want:

$$|P'| = \left| \overline{[P, P]} \right| \cdot |Q'| \leq p^{n-1} p^{(n-1)(n-2)/2} = p^{n(n-1)/2}$$

[4A.11]

Throughout we implicitly use that A is Abelian to reorder products. Let $f : H \rightarrow A$ be an arbitrary element of B , and let $k \in K$. Then note that

$$[f, k](h) = f(h)^{-1} f(hk^{-1})$$

This is enough to imply, for any $h \in H$,

$$\prod_{x \in hK} ([f, k](x)) = \prod_{x \in hK} f(x)^{-1} \prod_{x \in hK} f(xk^{-1}) = 1$$

where the last equality follows from the fact that as x iterates over hK , so does xk^{-1} . Let T be a transversal for K in H . If we then define

$$N := \left\{ f : H \rightarrow A \mid \forall t \in T, \prod_{x \in tK} f(x) = 1 \right\}$$

We've shown that $[B, K] \leq N$. We now work to show that $N \leq [B, K]$.

To that end, let $f \in N$. For $k \in K$ define the function $g_k : H \rightarrow A$ as

$$g_k(x) = \begin{cases} f(x) & xk \in T \\ 1 & xk \notin T \end{cases}$$

Now we define $g \equiv \prod [g_k, k]$, where the product is over $k \in K$. We claim $g^{-1} = f$. To see this, first let $x \in H \setminus T$, with $x = tr$, $r \neq 1$. Then $g_k^k(x) = 1$ for all $k \in K$ while $g_k(x) = f(x)$ precisely when $k = r^{-1}$, and is trivial otherwise. Thus indeed $g(x) = f(x)^{-1}$. But $g \in N$ by the first part of this solution, and thus $g(t)$ for $t \in T$ is determined by the values of $g(tk)$ for $1 \neq k \in K$. So we have $g \equiv f^{-1}$ and we've shown that $N = [B, K]$. Note that for $f \in N$, the values on $H \setminus T$ are arbitrary, and they determine the values on T . Hence

$$|N| = |A|^{|H|-|T|} = |A|^{|H|-[H:K]}$$

[4A.12]

- (a) Write $x = bh$ and $y = ck$ with $b, c \in B$ and $h, k \in H$. Since $[x, y] \in B$, we see that in the quotient $\overline{G} := G/B$ we have

$$1 = [\overline{x}, \overline{y}] = [\overline{h}, \overline{k}] = \overline{[h, k]}$$

Thus $[h, k] \in H \cap B = \{1\}$, so that h and k commute; pick a $T \in \mathcal{T}(H)$ containing $\langle h, k \rangle$, meaning $x, y \in BT$. Then $[B, T] \triangleleft BT$; in the corresponding quotient $\overline{B}$ and $\overline{T}$ commute. Since $\overline{B}$ and $\overline{T}$ are Abelian, the quotient is then Abelian, meaning

$$[\overline{x}, \overline{y}] = [\overline{x}, \overline{y}] = 1$$

so that $[x, y] \in [B, T]$.

- (b) By part (a) all commutators in $G' \cap B$ are contained in $[B, T]$ for some $T \in \mathcal{T}(H)$. Thus the number of commutators is bounded above by

$$\left| \bigcup_{T \in \mathcal{T}(H)} [B, T] \right| \leq \sum_{T \in \mathcal{T}(H)} |A|^{|H|-[H:T]} = |A|^H \sum_{T \in \mathcal{T}(H)} |A|^{-[H:T]}$$

where the first inequality follows from the previous problem, determining $|[B, T]|$. By the hypothesis of the problem, that last number is strictly less than $|A|^{|H|-1}$, which by the previous problem is $|[B, H]|$. We see then that in this case, not every element in $[B, H] \leq G' \cap B$ is a commutator.

(c) By hypothesis, $[H : T] \geq 2$ for all $T \in \mathcal{T}(H)$. Let $m = |\mathcal{T}(H)|$. Then we have

$$\sum_{T \in \mathcal{T}(H)} |A|^{-[H:T]} \leq \sum_{T \in \mathcal{T}(H)} |A|^{-2} = m|A|^{-2}$$

When $|A| > m$, then that rightmost expression is strictly less than $|A|^{-1}$, so the inequality of part (b) holds. If $H = D_8$, then it has 3 Abelian subgroups of order 4, so we can indeed take $m = 3$. Note that if A is cyclic of order 4 then $A \wr H$ has order 2^{19} in this case, giving a 2-group where not every element in the commutator subgroup is a commutator.

[4A.13] We prove by induction that for $k > 1$, we have $\gamma^k(H) \leq \gamma^{k+1}(G)$. Since $\gamma^{m+1}(G) = \{1\}$, we then have that H has nilpotence class less than m . For the base case $k = 2$, note that $\gamma^3(G) \leq G'$ is normal in H , and in the quotient $\bar{H} := H/\gamma^3(G)$, we see that $\overline{\gamma^2(G)}$ is central. But $\bar{H}/\overline{\gamma^2(G)}$ is a quotient of the cyclic group $\langle a \rangle$, implying that $\bar{H}$ is Abelian. Thus $\gamma^2(H) \leq \gamma^3(G)$.

For the inductive step, we simply have

$$\gamma^{k+1}(H) = [\gamma^k(H), H] \leq [\gamma^{k+1}(G), G] = \gamma^{k+2}(G)$$

4B

[4B.1] Assume G has nilpotence class $m > 2$, and choose k to be the smallest integer with $2k \geq m + 1$. We define $A = \gamma^k(G)$. We chose k such that

$$[A, A] = [\gamma^k(G), \gamma^k(G)] \leq \gamma^{2k}(G) \leq \gamma^{m+1}(G) = \{1\}$$

implying A is Abelian. If A was central, then $\gamma^{k+1}(G)$ is trivial, implying $k \geq m$. Because k was chosen as the smallest integer satisfying our inequality, this implies

$$2(m-1) < m+1$$

which is equivalent to $m < 3$. This contradicts the hypotheses, so A is non-central, and of course its characteristic.

Note that Q_8 has no characteristic Abelian non-central subgroups, so the condition on m is necessary.

[4B.2] If G has nilpotence class at most 2, then we can take $K = G$. So we assume that the nilpotence class of G is $m > 2$. By the previous problem, we know G has non-central characteristic Abelian subgroups; let $A \leq G$ be a maximal such one. If $C_G(A) = A$, then we're done. So we further assume that $K := C_G(A)$ strictly contains A ; note K is characteristic in G . If K has nilpotence class larger than 2, then the previous problem again shows K has a maximal non-central characteristic Abelian subgroup $B \leq K$. Since B is

non-central, $A < B$ (A is contained in B by maximality of B). But B is characteristic in G , and this contradicts the maximality of A . Thus K has nilpotence class at most 2. Also since $A \leq K$ we see that

$$C_G(K) \leq C_G(A) = K$$

So $K \leq G$ is our desired subgroup in this final case.

[4B.3] We fix j and prove this by induction on i . The base case $i = 1$ is by definition: $[G, Z_j] \leq Z_{j-1}$ since Z_j/Z_{j-1} is central in G/Z_{j-1} . Now we assume the inductive hypothesis, and note that

$$[Z_j, G, G^{i-1}] = [G, Z_j, G^{i-1}] \leq [Z_{j-1}, G^{i-1}] \leq Z_{j-i}$$

where the last containment follows from the inductive hypothesis. Similarly,

$$[G^{i-1}, Z_j, G] \leq [Z_{j-i+1}, G] \leq Z_{j-i}$$

where the first containment follows from the inductive hypothesis. The Three Subgroups Lemma then shows

$$[G^i, Z_j] = [G, G^{i-1}, Z_j] \leq Z_{j-i}$$

completing the proof.

[4B.4]

- (a) Since Y centralizes $[X, Y]$, we have $[X, Y, Y] = [Y, X, Y] = 1$. The Three Subgroups Lemma then shows $[Y, Y, X] = 1$, so that $Y' = [Y, Y]$ centralizes X .
- (b) There's no loss in assuming $G = XY$, so that $Z := [X, Y] \triangleleft G$. Then $[Z, X] \leq Z$ and $[Z, Y] = \{1\}$. This means $[Z, X, Y] = [Y, Z, X] = 1$. The Three Subgroups Lemma then shows

$$[Z, Z] = [X, Y, Z] = \{1\}$$

so that Z is Abelian.

[4B.5] By Theorem 4.15, we just need to show G contains a self-centralizing normal subgroup. Let $A \triangleleft G$ be a maximal Abelian normal subgroup. We show $C_G(A) = A$, which solves the problem. Suppose instead that $C := C_G(A) > A$, and we reach a contradiction. Since $A \triangleleft G$ and $C \triangleleft G$, we know there's a minimal normal subgroup of G/A contained in C/A ; let it be B/A . By part (a) of [3B.7] B/A has prime order, hence is cyclic. Since $B \leq C$, we have $A \leq Z(B)$, so that B is actually Abelian. This contradicts the maximality of A , so that we must have A a self-centralizing subgroup after all.

4C

[4C.1] Note that by Corollary 4.21 we have $[H_i, A] \leq H_{i-1}$ for $0 < i \leq m$. In particular, this implies

4D

$[G, A]_m = \{1\}$. But $[G, A]_m$ is normal in $[G, A]_{m-1}$, and thus we have a chain of A -invariant subnormal subgroups

$$1 = [G, A]_m \triangleleft [G, A]_{m-1} \triangleleft \cdots \triangleleft [G, A] \triangleleft A$$

Again by Corollary 4.21 we see that A stabilizes this chain, and we're done.

[4C.2] As in the previous problem, we have $[H_i, A] \leq H_{i-1}$. We prove by induction that

$$[H_{m-i}, A^j] \leq H_{m-i-j}$$

for $0 < i + j \leq m$. This implies in particular that $[G, A^m] \leq H_0 = \{1\}$, so that A^m is trivial and A has nilpotence class at most $m - 1$.

We induct on j . The case $j = 1$ is in the solution of the previous problem: $[H_{m-i}, A] \leq H_{m-i-1}$. Now suppose it is true for all values less than j , and note that

$$\begin{aligned} [H_{m-i}, A^{j-1}, A] &\leq [H_{m-i-j+1}, A] && \text{(induction)} \\ &\leq H_{m-i-j} \\ [A, H_{m-i}, A^{j-1}] &\leq [H_{m-i-1}, A^{j-1}] \\ &\leq H_{m-i-j} && \text{(induction)} \end{aligned}$$

Since H_{m-i-j} is normal, the Three Subgroup lemma shows $[A^j, H_{m-i}] = [A^{j-1}, A, H_{m-i}]$ is contained in H_{m-i-j} , as desired.

[4C.3] Since N is normal, $[N, G] \leq N$. So we have

$$[N, G, A] \leq [N, A] = \{1\}$$

with the last equality because A acts trivially on N . In particular, $[N, A, G] = \{1\}$, so the Three Subgroups lemma shows $[G, A, N] = \{1\}$, which means $N \leq C_G([G, A])$, and we're done.

4D

[4D.1]

- (a) Since $[N, A] = 1$ we know that $N \triangleleft \Gamma := G \rtimes A$. If $ga \in \Gamma$ centralizes N , then so does g , so that $g \in C_G(N)$. Thus $C_\Gamma(N) = C_G(N)A$. Since $C_G(N) \leq N$ and $[N, A] = 1$, we have that $A \triangleleft C_\Gamma(N)$. Because $[C_\Gamma(N) : A] = |C_G(N)|$ divides $|N|$, it is coprime to $|A|$. Thus A is a normal (hence characteristic) Hall subgroup of $C_\Gamma(N)$. Since $C_\Gamma(N) \triangleleft \Gamma$, we see then that $A \triangleleft \Gamma$. But $G \triangleleft \Gamma$ so that

$$[G, A] \leq G \cap A = \{1\}$$

and thus A acts trivially on G .

- (b) Let $C := C_A(N) \leq A$. Since $|C_A(N)|$ divides $|A|$, from part (a) we know that $C_A(N) \leq C_A(G) = \{1\}$, and thus A acts faithfully on N .

[4D.2] We have that $a + b = ab\sqrt{[b, a]}$ by definition. Since $g + g^{-1} = gg^{-1} = 1$, we see that $-g = g^{-1}$. The last thing we need to note is that $[a^{-1}, b^{-1}] = (ab)[a, b](ab)^{-1} = [a, b]$ since $[a, b] \in Z(G)$. So we have

$$\begin{aligned}
 xy - yx &= xy(yx)^{-1}\sqrt{[(yx)^{-1}, xy]} \\
 &= [x^{-1}, y^{-1}]\sqrt{[x^{-1}, xy][y^{-1}, xy]} && ([\cdot, xy] \text{ homomorphism}) \\
 &= [x^{-1}, y^{-1}]\sqrt{[x^{-1}, x][x^{-1}, y][y^{-1}, x][y^{-1}, y]} && ([g, \cdot] \text{ homomorphism}) \\
 &= [x^{-1}, y^{-1}]\sqrt{[x^{-1}, y][y^{-1}, x]} \\
 &= [x, y]\sqrt{[x, y^{-1}][x, y^{-1}]^{-1}} && ([b, a]^{-1} = [a, b] = [a^{-1}, b^{-1}]) \\
 &= [x, y]
 \end{aligned}$$

[4D.3]

- (a) Since $|G|$ and $|A|$ are coprime, we know that for p dividing $|G|$ there is an A -invariant Sylow p -subgroup $P \leq G$. If $P \neq G$ then A acts trivially on P by hypothesis, so that $P \leq C_G(A)$. Doing this for all such primes p shows $G \leq C_G(A)$, contradicting that A acts non-trivially on G . Hence we must have $G = P$ is a p -group.
- (b) If $[G, A] < G$, then by hypothesis A acts trivially on $[G, A]$, so $[G, A] = [G, A, A] = 1$, contradicting that A acts non-trivially on G . Thus $[G, A] = G$. Since $G' < G$, and G' is characteristic, we know A acts trivially on G' . From $[G', A] = 1$ we get $[G, G', A] = 1$ and $[G', A, G] = 1$. The Three Subgroup lemma then shows

$$[G, G'] = [[A, G], G'] = [A, G, G'] = 1$$

so that $G' \leq Z(G)$.

- (c) A acts on $\overline{G} := G/G'$, and by Fitting's theorem we can write $\overline{G} = C \times D$ where C is points fixed by A and $D = [\overline{G}, A] = [\overline{G}, A]$. As in the previous part, if $[G, A] < G$ then $[G, A] = [G, A, A] = 1$ contradicts our hypothesis. Thus $[G, A] = G$ and $D = \overline{G}$. This is enough to imply $C = \{1\}$. If $G' < H < G$ is an A -invariant subgroup, by hypothesis we have $[H, A] = 1$ and thus $1 < \overline{H} \leq C$. This is a contradiction, and no such H can exist.
- (d) We have $G' \leq \Phi(G) < G$, so by the previous part $G' = \Phi(G)$ and G/G' is elementary Abelian.
- (e) By part (b) G has nilpotence class at most 2, so the map $[\cdot, y]$ with $y \in G$ is a homomorphism. By part (d) every p th power is in $G' \leq Z(G)$. Thus for any $x \in G$ we see

$$[x, y]^p = [x^p, y] = 1$$

Since $x, y \in G$ were arbitrary, the generators of G' all have order dividing p . Since $G' \leq Z(G)$ is Abelian, this means every element in G' has order p , so G' is elementary Abelian.

- (f) Assume p is odd. If $\Omega_1(G) < G$ then A acts trivially on all elements of order p , so Theorem 4.36 shows A acts trivially on G . This contradiction shows $\Omega_1(G) = G$. By part (b) and Theorem 4.8 every element in $\Omega_1(G)$ has order p , so this is true for G .
- (g) Let $g \in G$ be arbitrary. By part (d) $g^2 \in G'$. By part (e) then $g^4 = (g^2)^2 = 1$.

[4D.4] We work by induction on $|G|$, the case $|G| = 2$ being vacuous since $\text{Aut}(G)$ is trivial. For the inductive step, suppose A acts non-trivially on G . If $H < G$ is a proper A -invariant subgroup, then by induction A acts trivially on H . We are thus in the case of the previous problem, so that every element of G has order dividing 4 by part (g). The hypothesis then says A acts trivially on G , and this is our contradiction. So we've shown A acts trivially on G .

[4D.5] Note that by Fitting's theorem $B = C_B(A^{(n-1)}) \times [B, A^{(n-1)}]$. Because A (hence $A^{(n-1)}$) acts faithfully, we see $D := [B, A^{(n-1)}] > 1$. Also by coprimeness we have $[D, A^{(n-1)}] = D$. By repeated application of this fact, and since $A^{(n-1)} \leq G^{(i)}$ for $i \leq n-1$, we then have that $1 < D \leq G^{(i)}$. But then

$$1 < D = [D, A^{(n-1)}] \leq [G^{(n-1)}, G^{(n-1)}] = G^{(n)}$$

and thus the derived length of G is at least $n+1$. However, in $G/B \cong A$, the image of $G^{(n)}$ is contained in $A^{(n)} = \{1\}$, and so $G^{(n)} \leq B$. Since B is Abelian, this implies $G^{(n+1)} \leq [B, B] = \{1\}$, and G has derived length $n+1$.

If A has derived length n , choose a prime p not dividing $|A|$ and let C be a cyclic group of order p . Then with $G := C \wr A$ we have $G = B \rtimes A$ with $B = C^{|A|}$ having order coprime to $|A|$. Since A acts faithfully on B , we've just shown that G has derived length $n+1$.

[4D.6] We show that $\theta(G) = C_G(A)$; this is enough since

$$|\ker(\theta)| \cdot |\theta(G)| = |G| = |C_G(A)| \cdot |[G, A]|$$

Because the proof of Theorem 4.34 shows $[G, A] \leq \ker(\theta)$, we must have $[G, A] = \ker(\theta)$ if $\theta(G) = C_G(A)$. But as shown in the proof, for $g \in C_G(A)$ we have $\theta(g) = g^{|A|}$, and $n := |g|$ is coprime to $m := |A|$. Pick integers a, b such that $an + bm = 1$. Then

$$\theta(g^b) = g^{bm} = gg^{-an} = g$$

showing that $g \in \theta(G)$, as desired.

[4D.7] First suppose that $O_{p'}(G) = \{1\}$. Then $P \leq C_G(O_p(G)) \leq O_p(G)$ follows from P

being Abelian and the Hall-Higman theorem. Thus $P = O_p(G)$ is normal and self-centralizing in G . Now $C := P \cap N_G(K)$ normalizes K , so that by normality of P we have

$$[C, K] \leq P \cap K = \{1\}$$

Thus C centralizes K , and by hypothesis C is non-trivial. But C contains a subgroup of order p , which is the only subgroup of order p in P (because P is cyclic). Thus K centralizes the elements of order p in P , so by Corollary 4.35 K centralizes P . So $K \leq P$ which implies $K = \{1\}$.

If instead $O_{p'}(G) > 1$, then we can work in $\bar{G} := G/O_{p'}(G)$, where we know $O_{p'}(\bar{G}) = \{1\}$. $\bar{P}$ is still cyclic, and p still divides the order of $\bar{N}_G(K) \leq N_{\bar{G}}(\bar{K})$. From what was just proved $\bar{K} = 1$, so that $K \leq O_{p'}(G)$.

5A

[5A.1] Let T be a transversal for H in G . For $g \in G$ we have

$$v(g) = \prod_{t \in T} tg(t \cdot g)^{-1} = \prod_{t \in T} gt(t \cdot g)^{-1} = g^n \prod_{t \in T} t \prod_{t \in T} (t \cdot g)^{-1} = g^n$$

where the last equality follows from the fact that as t runs through T , so does $(t \cdot g)$.

[5A.2] We can pick $T = \{1\}$ as the transversal for G in G . So the pretransfer map $V(g) = g$ is the identity map. Then the transfer map v is just the identity composed with the quotient map, so it is the canonical map $G \rightarrow G/G'$.

[5A.3]

- (a) Suppose $st = \hat{s}\hat{t}$ for $s, \hat{s} \in S$ and $t, \hat{t} \in T$. Then $\hat{t}t^{-1} \in K$, so by definition of a transversal we have $t = \hat{t}$, and then of course $s = \hat{s}$.
- (b) Note that if $Hst = H\hat{s}\hat{t}$, then we would have $\hat{s}\hat{t}t^{-1}s^{-1} \in H$, implying $\hat{t}t^{-1} \in K$, so that $\hat{t} = t$ and thus (since S is a transversal for H in K) $\hat{s} = s$. So every right coset of H in G has at most one element of ST inside it. But for $g \in G$, we know we can write $g = kt$ for some $k \in K$ and $t \in T$. And we can write $k = hs$ for some $h \in H$ and $s \in S$. Thus $g = hst \in Hst$ and we see that every right coset of H intersects ST non-trivially. Thus ST is a transversal for H in G , and from part (a)

$$[G : H] = |ST| = |S| \cdot |T| = [G : K][K : H]$$

- (c) Let $ab \in ST$ be such that $Hstg = Hab$, so that $(st) \cdot g = ab$. Note this implies there exists $h \in H$ with $tgb^{-1} = s^{-1}ha \in K$, and thus $t \cdot g = b$. We thus have

$$s \cdot (tg(t \cdot g)^{-1}) = s \cdot (tgb^{-1}) = s \cdot (s^{-1}ha) = a$$

since $Hss^{-1}ha = Ha$. We have then shown

$$(st) \cdot g = ab = \left(s \cdot (tg(t \cdot g)^{-1}) \right) (t \cdot g)$$

- (d) We use the transversal ST for H in G to compute w . We also write $V_t(g) = tg(t \cdot g)^{-1}$ and $W_s = sg(s \cdot g)^{-1}$ to simplify notation below. We compute

$$\begin{aligned} w(g) &= \prod_{s \in S} \prod_{t \in T} (st)g[(st) \cdot g]^{-1} \\ &= \prod_{s \in S} \prod_{t \in T} (st)g[(s \cdot V_t(g))(t \cdot g)]^{-1} && \text{(part (c))} \\ &= \prod_{s \in S} \prod_{t \in T} s[tg(t \cdot g)^{-1}][s \cdot V_t(g)]^{-1} \\ &= \prod_{t \in T} \prod_{s \in S} sV_t(g)[s \cdot V_t(g)]^{-1} \\ &\equiv \prod_{t \in T} v(V_t(g)) \\ &= v\left(\prod_{t \in T} V_t(g)\right) && (v \text{ homomorphism}) \\ &= v(V_T(g)) \end{aligned}$$

[5A.4]

- (a) Note that $Hth = Hht = Ht$ so that $t \cdot h = t$. Then

$$v(h) = \prod_{t \in T} tht^{-1} = \prod_{t \in T} h = h^n$$

where we've used $h \in Z(G)$ a couple of times.

- (b) Let $h \in H$ be non-trivial, and suppose $|h| = m$. Since m and n are coprime, we can find integers $a, b \in \mathbb{Z}$ with $am + bn = 1$. Then

$$v(h^b) = h^{bn} = h^{1-am} = h(h^m)^{-a} = h$$

Thus v is surjective onto H , and hence v restricted to H is injective: $H \cap \ker(v) = \{1\}$. Both are obviously normal subgroups of G , so all that's left to show $G = H \times \ker(v)$ is to show that $H \ker(v) = G$. For arbitrary $g \in G$ suppose $v(g) = h$, with $|h| = m$ as above. Then

$$v(gh^{-b}) = v(g)v(h^b)^{-1} = hh^{-1} = 1$$

so that $g = (gh^{-b})h^b \in H \ker(v)$ and we're done.

[5A.5]

Let Γ be a group with $Z \leq Z(\Gamma) \cap \Gamma'$ such that $\Gamma/Z \cong G$. Choose $A \triangleleft \Gamma$ as the preimage of C . Since A/Z is cyclic and $Z \leq Z(\Gamma)$, we see A is Abelian. Also $\Gamma/A \cong G/C$ is cyclic; let $x \in \Gamma$ become a generator in Γ/A . Then by Lemma 4.6 the map $\theta : A \rightarrow \Gamma'$ given by

$\theta(a) = [a, x]$ is a surjective homomorphism with kernel $A \cap Z(G)$. Since $Z \leq A \cap Z(G)$, we thus have that $|Z|$ divides

$$|\ker(\theta)| = [A : \Gamma'] = [A/Z : \Gamma'/Z] = [C : G']$$

[5A.6] Let D be the dihedral group of order 2^n , with $C \leq D$ cyclic of order 2^{n-1} , and $t \in D \setminus C$ an involution acting by inversion on C . If $C = \langle c \rangle$, then $[c, t] = c^{-2}$ so we see $\langle c^2 \rangle \leq D'$. But $D/\langle c^2 \rangle$ is order 4, hence Abelian, so $D' \leq C$ has index 2. Since D/C is cyclic, the previous problem shows $M(D)$ has order dividing 2.

Now let E be the dihedral group of order 2^{n+1} , and let $z \in E$ be the unique element of order 2 in the cyclic index-2 subgroup of E . Then $Z = \langle z \rangle$ has order 2, and is normal (hence central). Also since E' contains all squares (as shown for D above), and since $|E| \geq 8$, we know that z is a square, and hence $Z \leq Z(E) \cap E'$. But $E/Z \cong D$, showing that $|M(D)| \geq |Z| = 2$. So we've shown that in fact $M(D)$ has order 2.

[5A.7] We follow the solution of [5A.5]. Let Γ be a group with $Z \leq Z(\Gamma) \cap \Gamma'$ such that $\Gamma/Z \cong G$. Choose $A \triangleleft \Gamma$ and $H \leq \Gamma$ with A a preimage of C and H a preimage of B , so that $\Gamma = AH$ and $A \cap H > Z$. Since Z is central and A/Z and H/Z are cyclic, we see A and H are Abelian, so that $A \cap H \leq Z(\Gamma)$. We thus have that $Z < A \cap Z(\Gamma)$. Lemma 4.6 then shows that

$$|Z| < |A \cap Z(\Gamma)| = [A : \Gamma'] = [A/Z : \Gamma'/Z] = [C : G'] = n$$

Choosing Γ where $Z \cong M(G)$ shows $|M(G)| < n$.

[5A.8]

- (a) Let G and H be groups with subgroups $M(A) \leq Z(G) \cap G'$ and $M(B) \leq Z(H) \cap H'$ with $G/M(A) \cong A$ and $H/M(B) \cong B$. Then $G \times H \rightarrow A \times B$ is surjective with kernel

$$M(A) \times M(B) \leq (Z(G) \times Z(H)) \cap (G' \times H') = Z(G \times H) \cap (G \times H)'$$

this shows that $|M(A) \times M(B)| = |M(A)| \cdot |M(B)|$ divides $|M(A \times B)|$.

- (b) We show that if Γ is a group with $Z \leq Z(\Gamma) \cap \Gamma'$ and $\Gamma/Z \cong A \times B$, then $|Z| \leq |M(A)| \cdot |M(B)|$. Combined with part (a) this shows $M(A \times B)$ has the same order as $M(A) \times M(B)$. The example in part (a) gives a $Z \cong M(A) \times M(B)$, and thus order considerations show $M(A \times B) \cong M(A) \times M(B)$.

So we have $\Gamma/Z \cong A \times B$; choose subgroups $C, D \triangleleft \Gamma$ with C a preimage of A and D a preimage of B . Let p be a prime dividing $|Z|$; by Corollary 5.4 we know that p divides $|A \times B| = |A| \cdot |B|$. Since $|A|$ and $|B|$ are coprime, p divides exactly one of them, say $|A|$. We can thus divide the primes dividing $|Z|$ into disjoint subsets π_A and π_B . Let Z_A be the normal Hall π_A subgroup, and similarly for Z_B , so that $Z = Z_A \times Z_B$. Since

$$[D : Z_A] = [D : Z][Z : Z_A] = |B| \cdot |Z_B|$$

is a π'_A number, $Z_A \triangleleft D$ is a normal (hence characteristic) Hall π_A -subgroup. The Schur-Zassenhaus theorem (and the fact Z_A is central) shows we can write $D = Z_A \times L$ for some normal (hence characteristic) subgroup of D . In particular, $L \triangleleft \Gamma$. We can do the same thing for C , writing $C = Z_B \times K$ with $K \triangleleft \Gamma$. Of course $K \cap L \leq C \cap D = Z$. Thus

$$K \cap L = (K \cap Z) \cap (L \cap Z) = Z_A \cap Z_B = \{1\}$$

We also have $CD = KZ_BZ_AL = Z_AKZ_BL = KL$, so that $\Gamma = K \times L$. Finally,

$$K/Z_A \cong (C/Z_B)/Z_A \cong C/Z \cong A$$

and similarly $L/Z_B \cong B$. Now $Z_A \leq Z(K) \cap (\Gamma' \cap K) = Z(K) \cap K'$, so that Z_A is a quotient of $M(A)$. Similarly Z_B is a quotient of $M(B)$, and we've shown

$$|Z| = |Z_A| \cdot |Z_B| \leq |M(A)| \cdot |M(B)|$$

5B

[5B.1] This problem is not correct as stated. Take $G = S_3$ and $P = A_3 = G'$. Then $P' = \{1\}$, so any 3-cycle $g \in P$ gives a counterexample. The errata for the book say the conclusion should be $g^t \in P$, so we prove that below.

By the Transfer Evaluation Lemma, and the fact g has order p , we know there is a subset $T_0 \subset T$ such that g acts trivially precisely on this set, and

$$1 = v(g) = \prod_{t \in T_0} tgt^{-1}$$

We can choose T such that $1 \in T$, and of course $1 \in T_0$. Now every term in this product belongs to P , so we're done as long as T_0 contains an element different from 1. But if $T_0 = \{1\}$, then $v(g) = g \in P'$, which contradicts our hypothesis. Thus a $t \neq 1$ belongs to T_0 , and as such does not belong to P , with $tgt^{-1} \in P$.

[5B.2] Let $X = \{x_1, \dots, x_m\}$, with $x_i^n = 1$ for all $1 \leq i \leq m$. Let s be a product of elements of X , and write

$$s = y_1 \cdots y_{k-1} x_1 y_{k+1} \cdots$$

where $y_j \in X \setminus \{x_1\}$ for $1 \leq j < k$. In other words, x_1 first appears in the k th position in s . Then we can write

$$s = x_1 y_1^{x_1} \cdots y_{k-1}^{x_1} y_{k+1} \cdots$$

Since $y_j \neq x_1$ for $1 \leq j < k$, we know $y_j^{x_1} \neq x_1 = x_1^{x_1}$. Of course the $y_j^{x_1} \in X$ since it's closed under conjugation. So we have not changed the second position of x_1 in s . Proceeding this way, we can "collect" all the x_1 factors of s at the front, without changing the product's length. Since $x_1^n = 1$, we thus have

$$s = x_1^{e_1} \cdots$$

with $0 \leq e_1 < n$. We can now play the same game with x_2 in whatever product of elements comes after the x_1 s in s , and we can bring them to rest right after the x_1 s. Continuing this way, we will have written s as

$$s = x_1^{e_1} \cdots x_m^{e_m}$$

with $0 \leq e_i < n$ for $1 \leq i \leq m$. Thus every element of $\langle X \rangle$ can be written like this, and there are only n^m such products (though some may be equal as elements of G), hence $|\langle X \rangle| \leq n^m$.

[5B.3] If $x \in N$, with $N \triangleleft G$ a finite normal group, then x has finite order (dividing $|N|$), and since N contains all conjugates of x , it has only finitely many conjugates.

Conversely, suppose X is the conjugacy class of x , and it is a finite set, with $x^n = 1$. Then every element of X has order n , and by the previous problem

$$|\langle X \rangle| \leq n^{|X|}$$

So $N := \langle X \rangle$ is a finite group. But N is the smallest subgroup containing X , so for $g \in G$ we have that N^g is the smallest subgroup containing $X^g = X$. This shows N is normal in G , and we're done.

5C

[5C.1] If $P \leq Z(N_G(P))$, then of course P is Abelian, so Theorem 5.18 shows $P \cap G' = \{1\}$. But then G/G' , as an Abelian group, has a normal p -complement, whose preimage is a normal p -complement in G .

[5C.2] Let C be a complement to $P \triangleleft N_G(P)$, given by the Schur-Zassenhaus theorem. Then V and U are C -invariant. We see that $|V/U| = 2$, so that C acts trivially on $V/U \leq P/U$. In other words, $[C, V] \leq U$. Fitting's theorem shows $V = [C, V] \times C_V(C)$, so we must have some non-trivial $v \in C_V(C)$. But then v is central in $N_G(P) = PC$, so by Theorem 5.18 we have $v \notin G'$, and thus $G' < G$. If we assume G is simple then it must be Abelian, and since P is non-trivial, G is cyclic of order 2.

[5C.3] By Corollary 5.19, the only possible Abelian Sylow 2-subgroups for G are elementary Abelian and the group $P := C_4 \times C_4 \times C_2$. But defining

$$V = \langle x \in P \mid x^2 = 1 \rangle$$

$$U = \langle x^2 \mid x \in P \rangle$$

we have $[V : U] = 2$ and both are characteristic in P , so by the previous exercise P is not an option. Thus the Sylow 2-subgroup of G is elementary Abelian.

[5C.4] Let $m = rs$, where r divides $|G'|$ and s divides $[G : G']$, so that they're relatively prime (this is all possible by Theorem 5.16). By Schur-Zassenhaus $G = G' \rtimes H$ where $H \cong G/G'$.

Since G' is cyclic, it has a subgroup K of order r , which is characteristic in G' , hence normal in G . Since H is cyclic, it has a subgroup L of order s . Then $KL \leq G$ has order m .

Now suppose A and B are subgroups of order m in G , where again $m = rs$. The subgroup $K \leq G'$ of order r is the unique subgroup of order r in G , and since r must divide $|A \cap G'|$ and $|B \cap G'|$, we see that $K \leq A \cap B$. By the Schur-Zassenhaus theorem we can write $A = KC$ and $B = KD$ for some subgroups $C \leq A$ and $D \leq B$ of order s . Since G/G' is cyclic, and the images of both A and B in the Abelianization have order s , we must have $AG' = BG'$. In this common group, G' is a normal cyclic Hall subgroup, so the complements (of order s) are conjugate. That is, there exists $g \in AG'$ with $C^g = D$ and thus

$$A^g = K^g C^g = KD = B$$

[5C.5] Suppose $A^g = B$ for some $g \in G$. Then B is normal in both P and P^g , and thus $P, P^g \leq N_G(B)$. Thus there exists $x \in N_G(B)$ with $P^g = P^x$, meaning $gx^{-1} \in N_G(P)$. But

$$A^{gx^{-1}} = B^{x^{-1}} = B$$

so that A and B are conjugate in $N_G(P)$.

If A is characteristic in P , then $A \triangleleft N_G(P)$, meaning that $A = A^g = B$.

[5C.6]

- (a) Let $W \leq Q$. Write $P = Q^g$ for some $g \in G$, and note this means $W^g \leq P$, so that by hypothesis $W^g = W$ with $g \in N_G(W)$. Now if $W^x \leq Q$ for some $x \in G$, we have $W^{xg} \leq P$, meaning that again we have $xg \in N_G(W)$, so that x normalizes W and $W^x = W$, as desired.
- (b) Suppose W is weakly closed in P . Then if $P^g = P$, we have $W^g \leq P$ so that $W^g = W$ and $g \in N_G(W)$. In other words, $N_G(P) \leq N_G(W)$, and W is normal in $N_G(P)$. By part (a) W is weakly closed in all Sylow p -subgroups containing it, so the previous reasoning shows it is normal in all the associated normalizers.

Conversely, suppose $W \leq P$, with $W \triangleleft N_G(P)$ and also normal in all Sylow p -subgroups that contain it. Now suppose $W^g \leq P$ for some $g \in G$. Then W is normal in both P and $P^{g^{-1}}$, so that both are contained in $N_G(W)$. There is thus $x \in N_G(W)$ with $P^x = P^{g^{-1}}$, so that $g = x^{-1}n$ for $n \in N_G(P)$. But then

$$W^g = W^{x^{-1}n} = W^n = W$$

since W is normal in $N_G(P)$. Thus W is weakly closed in P .

- (c) Let $Q \leq H$ be a Sylow p -subgroup of H containing W , with $Q \leq P$ for a Sylow p -subgroup $P \leq G$. Then W is weakly closed in P . Now if $W^g \leq H$, we have $W^g \leq Q^h$ for some $h \in H$, meaning that $W^g \leq P^h$, and thus $W^{gh^{-1}} \leq P$. This means $W^{gh^{-1}} = W$, and thus $W^g = W^h$.

- (d) Let $x, y \in P$ with $x^g = y$. Then y is centralized by both W and W^g so that both are contained in $C_G(y)$. By part (c) there's an $h \in C_G(y)$ with $W^g = W^h$. Then $gh^{-1} \in N_G(W)$ with

$$x^{gh^{-1}} = y^{h^{-1}} = y$$

[5C.7] Let $Q \leq G$ be a Sylow 5-subgroup. Since $|\text{Aut}(Q)| = 4$ and $|G|$ is odd, Q must be central in its normalizer by the N/C -theorem, so that G has a normal subgroup N of order $3^a \cdot 11$. But $11 \not\equiv 1 \pmod{3}$, so that N has a unique Sylow 3-subgroup P . Thus P is characteristic in N , hence normal in G .

[5C.8] Let $P \leq G$ be a Sylow p -subgroup for G , which must be Abelian by [1D.9]. Let $Q \leq N_G(P)$ be a Sylow q -subgroup with $p \neq q$. Then since all non-trivial orbits of Q acting on P have size divisible by q , we must have

$$|C_P(Q)| \equiv |P| \pmod{q}$$

But $C_P(Q) \leq P$ is a subgroup, so has order 1, p , or p^2 . But q cannot divide $p^2 - 1$ or $p^2 - p$ since $q > p + 1$ (here we use $p \neq 2$). Thus $C_P(Q) = P$; since this works for all Sylow subgroups of $N_G(P)$, we see P is central in its normalizer, and thus G has a normal p -complement.

[5C.9] Let $P \leq G$ be a Sylow 2-subgroup. As in the previous problem, let $Q \leq N_G(P)$ be a Sylow q -subgroup of odd order, and note

$$|C_P(Q)| \equiv |P| \equiv 4 \pmod{q}$$

If $C_P(Q) < P$, then since q is odd it must divide $4 - 1 = 3$, and thus $q = 3$ divides $|G|$. Otherwise $C_P(Q) = P$ for all Sylow subgroups of $N_G(P)$, meaning $P \leq Z(N_G(P))$ and G has a normal 2-complement, contradicting simplicity.

[5C.10] Let $P \leq G$ be a Sylow 2-subgroup of order 8, and let $C \leq N_G(P)$ be a 2-complement. By Theorem 5.18 we must have $C_P(C) = \{1\}$ since $G = G'$. Now the orbits of C acting on $P \setminus \{1\}$ are all of odd size larger than 1, so we have 7 expressed as a sum of positive odd integers all greater than 1. That can only happen in one way: $7 = 7$. Thus C has an orbit of size 7, meaning that 7 divides $|C|$, hence $|G|$.

[5C.11] Note that H is Abelian. We work by induction on $|G|$. If P is a Sylow p -subgroup of H and $N_G(P) < G$, then by induction $N_G(P)$ has a normal p -complement C . Since $C \cap P = \{1\}$, this means $N_G(P) = P \times C$, and thus P is central in its normalizer. This implies G has a normal p -complement.

Now suppose $N_G(P) = G$ and $Q \leq H$ is another Sylow q -subgroup of H (with $p \neq q$) such that $N_G(Q) < G$. The same inductive argument shows P is central in $N_G(Q)$, so that $N_G(Q) \leq C_G(P) \triangleleft G$. Frattini's argument then shows

$$G = C_G(P)N_G(Q) = C_G(P)$$

so that P is central in its normalizer, and G has a normal p -complement.

We are thus reduced to the case where every Sylow subgroup of H is normal in G . But then H is normal in G , hence by hypothesis $H \leq Z(G)$. Then every Sylow subgroup is central in its normalizer, and in this final case G has a normal p -complement for all p dividing $|H|$.

[5C.12] Let $Q \leq N$ be a Sylow p -subgroup, and let $P \leq G$ be a Sylow p -subgroup containing Q . We can of course assume that $G = PN$. Then $K := N \cap N_G(P)$ is normal in $N_G(P)$. Since P is cyclic, $Q < P$ is characteristic in P , so that $Q \triangleleft N_G(P)$ as well. The Schur-Zassenhaus theorem then gives $K = QC$ for a p -complement C . We have

$$[C, P] \leq [K, P] \leq K \cap P = Q < P$$

Fitting's theorem says $P = [C, P] \times C_P(C)$, and since P is cyclic, only of these two factors is non-trivial. The strict containment above then says $[C, P] = 1$ and $P = C_P(C)$. So P is central in

$$PC = PQC = PK = P(N \cap N_G(P)) = PN \cap N_G(P) = N_G(P)$$

This means G has a normal p -complement M . Since G/N is a p -group, we must have $M \leq N$, and this is then a normal p -complement of N .

[5C.13] We can assume $G = N_G(P')$. Then in G/P' , we see that P/P' is self-normalizing, so that by Burnside's theorem G/G' has a normal p -complement M/G' . In particular, G is p -solvable, as evidenced by the normal series

$$1 \leq P' \leq M \leq G$$

Now let H be a Hall p' -subgroup of G , so that $HP' = M \triangleleft G$ since both are subgroups containing P' that map to Hall p' -subgroups in the p -nilpotent group G/P' . Then for $g \in G$ we have $H^g \leq M$, so that there exists $x \in P'$ with $H^g = H^x$ by the Schur-Zassenhaus theorem applied to the solvable normal Hall subgroup $P' \leq M$. Thus $g = (gx^{-1})x$ belongs to $N_G(H)P'$, showing we must have $G = N_G(H)P'$. Dedekind's lemma shows

$$P = P'N_G(H) \cap P = P'(N_G(H) \cap P)$$

But $P' \leq \Phi(P)$ by [1D.8], meaning $P \leq N_G(H)$ by [1D.7], and thus $G = N_G(H)$. Thus $H \triangleleft G$ is our normal p -complement.

5D

[5D.1] Let $N \triangleleft H$ be a normal p -complement in H . Then note that $A^p(H) = N$ since $H/N \cong P$ is an Abelian p -group, and of course $N \leq A^p(H)$ since $|N|$ is coprime to p . Because H controls p -transfer in G , we know that $[G : A^p(G)] = [H : A^p(H)] = |P|$. Thus $|A^p(G)|$ is coprime to p and hence $A^p(G)$ is a normal p -complement.

[5D.2] Since $P \leq Z(G)$, we know $P \triangleleft G$, and hence by Schur-Zassenhaus G has a p -complement $M \leq G$. But P is central, so $P \leq C_G(M) \leq N_G(M)$. Thus $M \triangleleft G$ and G has a normal p -complement.

Now suppose $P \leq Z(N_G(P))$. Then P is Abelian, so by Corollary 5.23 $N_G(P)$ controls p -transfer in G . By the previous paragraph $N_G(P)$ has a normal p -complement. By the previous exercise, G does too.

[5D.3]

- (a) If $P < Q$ for Q a Sylow p -subgroup of G , then P could not be maximal. Thus P is a Sylow p -subgroup.
- (b) Let Q be a Sylow p -subgroup of G containing N , and let $M := P \cap Q$. Note that $M \triangleleft P$ since $P' \leq N \leq M$. Since normalizers grow, if $M < Q$, we have that $P < N_G(M)$, and maximality then implies $N_G(M) = G$. Since we're assuming N (hence M) is non-trivial, this contradicts the fact G is simple. So we must have $P = M = Q$, and so P is the only Sylow p -subgroup of G containing N .

Now by simplicity of G and maximality of P , we have $P = N_G(P)$. By the previous paragraph then, and part (b) of [5C.6], we see that N is weakly closed in P .

- (c) Suppose the nilpotency class of P is at most 2. Then $N = Z(P)$ is a non-trivial normal subgroup of P with P/N Abelian, so the previous part applies, and N is weakly closed in P . By part (d) of [5C.6], $N_G(N)$ controls p -fusion in G . But G is simple and P is maximal, so $N_G(N) = P$. But then P controls p -transfer, and from $A^p(P) = P' < P$ we see that $A^p(G) < G$, contradicting simplicity of G . So the nilpotency class of P must be at least 3.

[5D.4] Note the image of K in $G/O^p(G)$ is a p -group, meaning $K/(K \cap O^p(G))$ is a p -group, implying $O^p(K) \leq K \cap O^p(G)$ by definition. Now if $P \leq K$ is a Sylow p -subgroup of G , then we have $KO^p(G) = PO^p(G) = G$. This means $K'O^p(G) \triangleleft G$ and that the quotient $G/K'O^p(G)$ is a quotient of K/K' , hence Abelian. Thus $G' \leq K'O^p(G)$ and we have the equality

$$K'O^p(G) = G'O^p(G) = A^p(G)$$

Finally if we assume $O^p(K) = O^p(G) \cap K$, then we have

$$A^p(K) = K'O^p(K) = K'(O^p(G) \cap K) = K'O^p(G) \cap K = A^p(G) \cap K$$

[5D.5] Note that $P' = A \cap P$ is a Sylow p -subgroup of A . Since $P' \triangleleft A$, the Schur-Zassenhaus theorem shows there's a p -complement $K \leq A$. A Frattini argument shows $G = N_G(K)P'$. Namely, if $g \in G$, then $K^g \leq A$ since A is normal in G . Since P' is solvable and K^g is a p -complement in A , there exists $a = kp \in KP' = A$ with $K^g = K^a = K^p$. Then $g = (gp^{-1})p \in N_G(K)P'$. From Dedekind's lemma we have

$$P = N_G(K)P' \cap P = P'(N_G(K) \cap P)$$

Since $P' \leq \Phi(P)$ we must have $P \leq N_G(K)$, and thus $G = N_G(K)$. Now $|K|$ is coprime to p , but $[G : K] = [G : A][A : K]$ is a power of p , so that K is a normal p -complement.

[5D.6] Let $N = N_G(P')$, and note $P \leq N$. From $P' \leq A^p(N) \leq A^p(G) = A$, we have that $A^p(N) \cap P = P'$ and we are in the situation of the previous problem, so that N has a normal p -complement K and $N = K \times P'$. Since P' is Abelian, we have $P' \leq Z(N)$. But then P' is central in $N_A(P') \leq N$, and Burnside's theorem implies A has a normal p -complement C . Since C is characteristic in A , it is normal in G . Also $[G : C] = [G : A][A : C]$ shows C is a p -complement for G .

5E

[5E.1] Note if $N_G(X) < G$ for all non-trivial p -subgroups $X \leq G$, then by hypothesis $N_G(X)$ has a normal p -complement for all such X , and then Frobenius's theorem shows G has a normal p -complement. Since this contradicts our hypothesis, there must be some non-trivial X normal in G . In other words, $O_p(G) > 1$.

Let $H < G$ so that H has a normal p -complement $M \triangleleft H$. Then in $\overline{G} := G/O_p(G)$, we have $\overline{M}$ is a p' -group, while $[\overline{H} : \overline{M}]$ divides $[H : M]$; in other words, $\overline{M}$ is a normal p -complement in $\overline{H}$. So if $\overline{G}$ does not have a normal p -complement, we are in the situation of the previous paragraph, so that $\overline{K} := O_p(\overline{G}) > 1$. But then $K \triangleleft G$ is a normal p -subgroup properly containing $O_p(G)$, and that's a contradiction. Thus $\overline{G}$ has a normal p -complement $\overline{N}$, so that $N \triangleleft G$ has p -power index. If $O_p(G) < P$ then $N < G$ so that N has a normal p -complement $M \leq N$, which is then a normal p -complement in G :

$$[G : M] = [G : N][N : M]$$

This contradicts our hypotheses, so $O_p(G) = P$ and P is normal in G . Now let $\{q_1, \dots, q_r\}$ be the primes not equal to p dividing G , and let $Q_i \leq G$ be a Sylow q_i -subgroup. If $PQ_i < G$, then by hypothesis it has a normal p -complement, so Q_i is normalized (hence centralized) by P . If $r > 1$ then, $C_G(P)$ contains every Sylow q -subgroup for $q \neq p$, and thus $PC_G(P) = G$. If $C_G(P) < G$ we would have a normal p -complement in $C_G(P) \triangleleft G$, hence in G . So it must be that $C_G(P) = G$, and then Burnside's transfer theorem gives our final contradiction. We therefore must have $r = 1$, as desired.

[5E.2] Let G be a non-solvable group with every proper subgroup supersolvable, and choose G such that $|G|$ is minimal; we will reach a contradiction to show G does not exist. First, if $1 < N \triangleleft G$ is a proper normal subgroup, then N is solvable since it's proper, and G/N is solvable by the minimality hypothesis, so G would be solvable. Thus N does not exist, and G is simple.

Let p be the smallest prime divisor of $|G|$, and $X \leq G$ a nontrivial p -subgroup. Then $N_G(X) < G$ by simplicity, so it's supersolvable. Let $Q \leq N_G(X)$ be a Sylow q -subgroup,

with $q \neq p$. Then XQ is supersolvable, and by [3B.10] Q is normal in XQ because $q > p$. Since $X \triangleleft XQ \leq N_G(P)$ as well, we see that Q centralizes X . Since this works for all primes $q \neq p$, we have that $N_G(X)/C_G(X)$ is a p -group. We can then apply Frobenius's theorem to conclude G has a normal p -complement. But simplicity forces then G to be a p -group, hence Abelian. So it was solvable all along, and we have our final contradiction.

[5E.3] Suppose G satisfies the hypotheses, but does not have a normal p -complement, and it is minimal in terms of order; since every proper subgroup also satisfies the hypotheses, they all must have a normal p -complement by minimality. By [5E.1] we have a normal Sylow p -subgroup $P \triangleleft G$ and we can write $G = PQ$ for a Sylow q -subgroup Q . Now let $x \in P$ and $y \in Q$; by hypothesis, $Z := \langle x, y \rangle$ has a normal p -complement, while $P \cap Z \triangleleft Z$ is a normal Sylow p -subgroup. In particular Z is the direct product of its Sylow p -subgroup Z_p and Sylow q -subgroup Z_q . Since $x \in Z_p$ and $y \in Z_q$, we have that x and y commute. Since x and y were arbitrary, we see that P and Q commute, so that $Q \triangleleft G$. This would be a normal p -complement, and this contradiction shows G does not exist. Thus all such groups have normal p -complements.

6A

[6A.1] Let $a \in A$ be non-trivial. If a fixed a non-zero vector $v \in V$ (here V is the vector space of order p^2), then we can complete to a basis $\{v, w\}$ of V , in which a would have matrix form

$$a = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$$

The first row comes from fixing v , while the bottom row comes from $\det(a) = 1$ (here $x \in \mathbb{F}_p$). It's easy to see from $px = 0$ that $a^p = 1$, so that a has order p . This contradicts our hypothesis, so a has no non-zero fixed vectors. Since $a \in A \setminus \{1\}$ was arbitrary, this shows A acting on V is a Frobenius action.

[6A.2] We write $\{v_1, v_2, v_3\}$ as the basis for $V = F^3$ giving the matrices for a and b , such that

$$a(v_i) = \alpha^{2^i} v_i \quad b(v_i) = \begin{cases} v_{i+1} & i \neq 3 \\ \epsilon v_1 & i = 3 \end{cases}$$

Clearly $|a| = 7$ and $|b| = 9$ since $b^3(v) = \epsilon v$. Note also that

$$b^{-1}ab(v_1) = b^{-1}a(v_2) = b^{-1}(\alpha^4 v_2) = \alpha^4 v_1$$

And similarly for v_2 and v_3 , so that $b^{-1}ab(v_i) = \alpha^2(v_i)$. This shows b normalizes $\langle a \rangle$, so we get that $A = \langle a, b \rangle$ has order 63. Since $a^b \neq a$ we see A is non-Abelian. Finally, we show that A acts on V with a Frobenius action. Note that if $a \in A$ was non-trivial and fixed

a non-zero $v \in V$, then some power of a would have prime order, and also fix v . So it's enough to show no element of prime order in A fixes any such v .

The elements of order 7 in A are of the form a^k for $0 < k < 7$. But

$$a^k(xv_1 + yv_2 + zv_3) = \alpha^{2k}xv_1 + \alpha^{4k}yv_2 + \alpha^kzv_3$$

And this can't be a fixed point as long as one of x, y, z is non-zero, because none of the powers of α are equal to 1. The elements of order 3 in A are conjugates of b^3 , so it's enough to show b^3 fixes no non-zero vectors. But $b^3(v) = \epsilon v$ makes this clear, and we're done.

[6A.3] Mimicking the previous problem, we choose $p = 221$ as a prime congruent to 1 (mod 55), with F the field of order p . Now let $\alpha \in F$ have order 11, and $\beta \in F$ have order 5. We define $a, b \in GL(5, p)$ according to a basis $\{v_1, \dots, v_5\}$ as follows:

$$a(v_i) = \alpha^{4i}v_i \quad b(v_i) = \begin{cases} v_{i+1} & i \neq 5 \\ \beta v_1 & i = 5 \end{cases}$$

As before, $|a| = 11$ and $|b| = 25$ since $b^5(v_i) = \beta v_i$. We also have that $b^{-1}ab(v_i) = a^4(v_i)$ so that b normalizes $\langle a \rangle$, and thus $A = \langle a, b \rangle$ has order $5^2 \cdot 11$. Also as before, we check the elements of prime order in A to see A has a Frobenius action on $V = F^5$. The same reasoning in the previous problem shows a^k has no non-zero fixed points for $0 < k < 11$, and also that b^5 has no non-zero fixed points either.

[6A.4] Let A be a Frobenius complement in G , and let our coset be aN for $1 \neq a \in A$. By [\[1D.4\]](#) (or Theorem 6.4) we see that $C_N(a) = \{1\}$, so that there are $|N|$ conjugates of a by N . But $[a, n] \in N$ for all $n \in N$ because N is normal. Thus $a^n \in aN$ for all $n \in N$. Since $a^N = |N| = |aN|$, we thus have that $aN = a^N \subset a^G$, so that aN is contained in the conjugacy class of a .

[6A.5] Because G is solvable, $F(G) > 1$ (it contains any minimal (Abelian) normal subgroup). Suppose p divides $|F(G)|$, and let $x \in Z(O_p(G)) \leq F(G)$ be non-trivial. Then because $F(G)$ is nilpotent, we have $F(G) \leq C_G(x)$, which is Abelian by hypothesis. Thus $F(G)$ is Abelian, and so $F(G) < G$ by hypothesis. For any $1 \neq y \in F(G)$, we thus have $F(G) \leq C_G(y)$, which is Abelian. Thus

$$C_G(y) \leq C_G(F(G)) \leq F(G)$$

with the last containment coming from [\[3B.14\]](#). If we can then show $F(G)$ has a complement in G , Theorem 6.4 will show G is a Frobenius group with kernel $F(G)$.

But for a prime q dividing $|F(G)|$, choose $g \in F(G)$ of order q , and let Q be a Sylow q -subgroup of G . Then $Z(Q) \leq C_G(g) \leq F(G)$. If $z \in Z(Q)$ is non-trivial, then $Q \leq C_G(z) \leq F(G)$. Thus $F(G)$ contains a Sylow q -subgroup of G for every prime q dividing $|F(G)|$, so that $F(G)$ is a normal Hall subgroup. The Schur-Zassenhaus theorem then shows $F(G)$ is complemented in G , and we're done.

It is a theorem of Suzuki that a finite group where every non-trivial centralizer is Abelian (called a CA-group) is solvable. Together with this problem, we see that such a group is either Abelian or a Frobenius group with kernel $F(G)$. Let A be a Frobenius complement in G . Since A is also a CA-group, we see the same dichotomy applies to A . As we'll see later (Theorem 6.9), it's impossible for A to be a Frobenius group, so that it must be Abelian. Again Theorem 6.9 implies A is cyclic. So CA-groups are Abelian groups, or Frobenius groups $K \rtimes C$ with K Abelian and C cyclic. It's easy to see (with results of this section) that all such groups are CA-groups, so this is a complete characterization. We'll finish this aside by noting the non-Abelian case does arise: consider S_3 or A_4 for example (both CA-groups).

[6A.6] Suppose $A \cap B^g = \{1\}$ for all $g \in G$, and we'll reach a contradiction. This implies that $A^g \cap B^h = \{1\}$ for all $g, h \in G$. Write $A_* = A \setminus \{1\}$ and similarly for B_* . Then $\{A_*, A_*^g, \dots, B_*, B_*^g, \dots\}$ is a finite collection of sets, all disjoint (here we're taking all conjugates of A_* and B_*). By Lemma 6.5, the number of elements in $\sqcup A_*^g$ is $|G| - [G : A]$, and similarly for $\sqcup B_*^g$. Since the identity is outside all of these sets, we have

$$\begin{aligned} |G| &> |G| - [G : A] + |G| - [G : B] \\ |G| &< [G : A] + [G : B] \\ &\leq |G|/2 + |G|/2 \\ &= |G| \end{aligned} \quad (A, B > 1)$$

This contradiction shows $A \cap B^g > 1$ for some $g \in G$.

[6A.7]

(a) Of course $A^g \cap H > 1$ satisfies the hypotheses of Lemma 6.5, since we have

$$(A^g \cap H) \cap (A^g \cap H)^h = A^g \cap A^{gh} \cap H$$

and if this is non-trivial, we must have $h \in A^g$ so that $h \in A^g \cap H$. Because $A \leq H$, by the previous problem (with $B = A^g \cap H$) there is some $h \in H$ with $A^h \cap (A^g \cap H) > 1$. Then $g \in A^h \leq H$ by the hypothesis on $A \leq G$.

(b) If $H \triangleleft G$, then for all $g \in G$, we have $A^g \cap H = A^g \cap H^g = A^g$. Since $H \geq A^g > 1$ the previous part shows $g \in H$. But $g \in G$ was arbitrary, so $H = G$.

[6A.8]

If $M \not\leq X$, then we must have $M \cap A^g > 1$ for some $g \in G$. Since $M \triangleleft G$, we have $M \cap A^g > 1$ for all $g \in G$. By part (a) of the previous problem applied to AM , we then see that $g \in AM$ for all $g \in G$, so that $AM = G$.

Since $A \cap M$ satisfies the hypothesis of Lemma 6.5, let $Y \subset M$ be the elements not conjugate into $A \cap M \setminus \{1\}$. Then $Y \subset X$ since if $1 \neq m \in M$ is such that $m^g \in A$, then $m^g \in A \cap M$ because M is normal in G . But we have by Lemma 6.5

$$|Y| = [M : A \cap M] = [AM : A] = [G : A] = |X|$$

Thus $X = Y \subset M$.

[6A.9] We remark first that by the proof of Theorem 6.4, we have $C_G(a) \subset A$ for $1 \neq a$ in A . This also follows from $C_G(a) \leq N_G(\langle a \rangle)$, which is contained in A by part (a) of [1D.3].

(a) Let $g \in G \setminus A$, and consider $D = \langle t, t^g \rangle$, which is a dihedral group. But

$$Z(D) \leq C_G(t) \cap C_G(t^g) \leq A \cap A^g = \{1\}$$

So that $1 \neq tt^g$ is inverted by t . Of course $tt^g \notin A$ since $g \notin A$. Now $tt^g = tt^h$ implies $gh^{-1} \in A = N_G(A)$. Since A has $[G : A]$ conjugates, this implies there are $[G : A] - 1$ distinct products like tt^g that t inverts.

(b) If t inverts $b \in A^g$, then $A^g \cap A^{gt} > 1$, so that $t \in A^g$. This implies $g \in A$. Thus the $[G : A] - 1$ elements of the previous part cannot lie in any non-trivial conjugate of A , and they don't live in A by construction. Thus t inverts $[G : A] - 1$ non-trivial elements of X . But X has $[G : A]$ elements, and contains the identity, so t must invert every element of X .

(c) If $r \in A$ was another involution, then by the previous part r inverts all elements of X . If $1 \neq x \in X$, then $x^{rt} = x$ so that $x \in C_G(rt) \leq A$, a contradiction. Thus r does not exist. So t is the unique involution in A , and thus $t^a = t$ for all $a \in A$, showing $t \in Z(A)$.

(d) If $x \in X$ had order $2m$, then $(x^m)^t = x^m$, so $x^m \in C_G(t) \leq A$. Since x^m is an involution, by the previous part $x^m = t$. Thus t centralizes x , again implying $x \in A$, which is a contradiction. Thus every element in X has odd order.

(e) If $xy^{-1} \in A$, then since $t \in Z(A)$ we have

$$x^{-1}y = x^t y^{-t} = (xy^{-1})^t = xy^{-1}$$

Thus $x^2 = y^2$. Because $|x|$ and $|y|$ are odd, we have $|x| = |x^2| = |y^2| = |y|$. Call this common order k , and choose n such that $2n \equiv 1 \pmod{k}$. Then

$$x = x^{2n} = (x^2)^n = (y^2)^n = y^{2n} = y$$

(f) We apply the subgroup test: for $x, y \in X$ we want $xy^{-1} \in X$. But if $xy^{-1} \notin X$, then $xy^{-1} \in A^{g^{-1}}$ for some $g \in G$. By the previous part

$$x^g y^{-g} = (xy^{-1})^g \in A \implies x^g y^{-g} = 1$$

Here we're relying on $x^g, y^g \in X$ because X is closed under conjugacy. Thus $(xy^{-1})^g$ (and hence xy^{-1}) is trivial (so still in X). Thus we always have $xy^{-1} \in X$ and we're done.

[6A.10]

- (a) By part (b) of [1D.3] A is a Hall subgroup, so contains a full Sylow p -subgroup of G for every prime p dividing $|A|$. Let $P \leq A$ be a Sylow p -subgroup. If $x \in P$ is such that $x^g \in P$ for $g \in G$, then $x^g \in A \cap A^g$, implying $g \in A$. Thus A controls fusion in P .
- (b) Note that $A \leq G'A \triangleleft G$, so by part (b) of [6A.7] we have $G'A = G$. Now clearly $A' \leq G' \cap A$. We show equality by showing that every Sylow p -subgroup $Q \leq G' \cap A$ is contained in A' . Let $P \leq G$ be a Sylow p -subgroup containing Q , and note that by part (a) $P \leq A$. We then have

$$Q = P \cap G' = \text{Foc}_G(P) = \text{Foc}_A(P) = P \cap A'$$

Here we've used the Focal Subgroup Theorem (5.21) as well as the fact that A controls fusion in P .

- (c) We proceed by induction on the derived length of A . First, if A is Abelian, then $A' = \{1\}$, so we see from part (b) that A is a complement to G' . By Corollary 6.6, $X = G'$ is a subgroup.

Now assume the theorem is true for all groups of derived length $\leq n$, and let A have derived length $n + 1$. Now $A' = G' \cap A \leq G'$ satisfies the hypothesis of Lemma 6.5, say with corresponding subset $Y \leq G'$. As in the solution to [6A.8], $Y \subset X$, and we have

$$|Y| = [G' : G' \cap A] = [G'A : A] = [G : A] = |X|$$

so that $Y = X$. Since A' has derived length n , the induction hypothesis shows Y is a subgroup, and we're done.

[6A.11] If A satisfies the hypothesis of Lemma 6.5, then by part (a) of [1D.3] we have $N_G(T) \leq A$ for all $1 < T \leq A$. Conversely, if $N_G(T) \leq A$ for all $1 < T \leq A$, then by [1D.5] we see A satisfies the hypothesis of Lemma 6.5.

6B

[6B.1] Let G be a Frobenius group with kernel N and complement A . Let $Q \leq A$ be a Sylow q -subgroup of A , and note that the action of Q on N is Frobenius. Since Q is solvable and $|Q|$ and $|N|$ are coprime, Glauberman's Lemma (more precisely Theorem 3.23) shows there exists a Sylow p -subgroup $P \leq N$ which is fixed by Q . Then PQ is a Frobenius subgroup of G by Theorem 6.4, and is clearly solvable.

Now if C is a Frobenius complement, and it contained a Frobenius subgroup G , by the above it would contain a solvable Frobenius subgroup. This contradicts Theorem 6.9 however, so the subgroup G does not exist.

[6B.2] Let p be a prime divisor of $|N|$, and let $P \leq A$ be a Sylow p -subgroup. If we let

$C := C_N(P)$, then C is A -invariant because A is Abelian. Specifically, if $c \in C$ and $a \in A$, for any $x \in P$ we have

$$(c^a)^x = c^{ax} = c^{xa} = (c^x)^a = c^a$$

so that $c^a \in C$ by definition. Letting P act on N shows $|N| \equiv |C| \pmod{p}$, and since $1 \in C$ we see $C > 1$. By hypothesis then, $C = N$, and faithfulness of A shows $P = 1$. Doing this for all primes dividing $|N|$ shows $|N|$ and $|A|$ are coprime. Since by hypothesis there are only two (trivial) A -invariant subgroups of N , Lemma 6.20 shows A is cyclic.

[6B.3] Let $N := \langle x \rangle$ be the cyclic group of order 8, and let $A = \langle a, b \rangle$ be the non-cyclic group of order 4, with action

$$x^a = x^3 \quad x^b = x^5$$

so that $x^{ab} = x^{-1}$. Then $C_N(a) = C_N(ab) = \langle x^4 \rangle$, while $C_N(b) = \langle x^2 \rangle$. Thus

$$\langle C_N(z) \mid 1 \neq z \in A \rangle = \langle x^2 \rangle < N$$

And this is a counterexample to Theorem 6.21.

[6B.4]

- (a) Let $x \in X$ for $X \in \Pi$. Then every element $X \neq Y \in \Pi$ is contained in $C_G(x)$. Fix such a Y and choose non-trivial $y \in Y$. Then $xy \notin X$, so that by hypothesis X centralizes xy . But X already centralizes y , so that $X \leq C_G(x)$, and thus $G = C_G(x)$. Since x and X were arbitrary, this shows G is Abelian.
- (b) Let $X \neq Y$ be two elements of Π , with nontrivial elements $x \in X$ and $y \in Y$. Suppose that $m := |x| \leq |y|$. Then we have

$$(xy)^m = x^m y^m = y^m$$

But xy is in some $Z \neq Y$, so that $(xy)^m \in Z \cap Y = \{1\}$. Thus $|y| \leq m$ and we see $|x| = |y|$. Now let p divide $|X|$ and choose $x \in X$ of order p . By the above reasoning applied to the case $|x| \leq |y|$ or $|y| \leq |x|$, we see that every element of Y has order p . Swapping X and Y shows every element of X has order p . Since X and Y were arbitrary, this shows every nontrivial element of G has order p . Together with part (a), this shows G is elementary Abelian.

[6B.5] We work via induction on $|G|$, the case $|G| = 1$ being trivial. If $H < G$ is not contained in any element of the partition Π , then $\{H \cap X\}_{X \in \Pi}$ is a partition of H by subnormal subgroups, so by induction H is nilpotent.

Let $X \in \Pi$ be such that $X \not\leq F(G)$, and let $M \leq G$ be a maximal subgroup containing X . If $M \neq X$, then by the preceding argument we have that M is nilpotent, so that X is nilpotent too. But since X is subnormal, we would have $X \leq F(G)$, a contradiction. So $M = X$, and since X is subnormal, we see X is a normal maximal subgroup of G . In particular we have $[G : X] = p$ is a prime number.

We now show such an X cannot exist, so that $G = F(G)$ is nilpotent. If X exists, and there's another $Y \in \Pi$ with $Y \not\leq F(G)$, then $G = XY$ with $X \cap Y = \{1\}$ shows $G = X \times Y$ with $|Y| = [G : X] = p$ and similarly $|X| = [G : Y] = q$ for some prime q . Thus G is Abelian, contradicting that $G \neq F(G)$. So all $Y \in \Pi$ with $X \neq Y$ are such that $Y \leq F(G)$. But then $G = X \cup F(G)$ is a contradiction, as no nontrivial group is the union of two proper subgroups.

[6B.6] Let $C = \langle x \rangle$ be a cyclic group of order 2^n with $n > 2$, and α an automorphism of order 2. Thus $\alpha(x) = x^r$ with $r^2 \equiv 1 \pmod{2^n}$. By Lemma 6.16 we have $r = -1$ or $r = 2^{n-1} \pm 1$. Since $n > 2$ all three of these choices are distinct, and all give automorphisms of order 2.

[6B.7] Let $\langle x \rangle = C \triangleleft P$ be the cyclic subgroup of index 2. Since P is non-Abelian, we must have $Z(P) < C$ (since otherwise $P = CZ(P)$ would be Abelian). Since $[P : Z(P)] > 4$ we know that $|P| > 8$, so that $|C| > 4$. Let $\alpha \in P \setminus C$ so that α induces an automorphism of order 2 on C (it cannot centralize C since then $Z(P) = C$ would have index 2). By the previous problem, we have $x^\alpha = x^{-1}$ or zx^{-1} or zx with $z \in C$ of order 2. By Lemma 6.13, we're done if we can rule out $x^\alpha = zx$.

But if $x^\alpha = zx$ then $(x^2)^\alpha = x^2$, so that $x^2 \in Z(P)$, which implies $[P : Z(P)] \leq 4$. This is a contradiction.

[6B.8] We work by induction on $|P|$, the case $|P| = 8$ being Corollary 6.14. Let $Z \leq Z(P) \cap P'$ have order 2. Since we have

$$[P/Z : (P/Z)'] = [P/Z : P'/Z] = [P : P'] = 4$$

our inductive hypothesis shows P/Z has a cyclic subgroup of index 2. Since Z is central, the preimage of this cyclic subgroup is an Abelian subgroup $A \leq P$ of index 2. Since A/Z is cyclic, we have that either A is cyclic or $A = C \times Z$ with C cyclic. By Lemma 4.6 we have $A \cap Z(P) = Z$ since $|A| = 2|P'|$. If $Z < Z(P)$ then we'd have $P = AZ(P)$ and P would be Abelian. Thus we must have $Z(P) = Z$.

If A is cyclic, then since we can assume $|P| > 8$, we have $[P : Z(P)] > 4$, so the previous problem shows P is dihedral, semidihedral, or generalized quaternion. If $A = C \times Z$, then since $|C| \geq 4$ we have a unique involution $t \in C$, which is the unique involution in A that has a square root. Thus $\langle t \rangle$ is characteristic in A , hence normal in P . But then $t \in Z(P) \setminus Z$, and that is a contradiction. Thus the A non-cyclic case does not occur, and we're done.

[6B.9] Suppose G is as in the problem, and that $|G|$ is not a p -group. We work via induction on $|G|$. Let $N \triangleleft G$ be a minimal normal subgroup, with $|N| = p^a$. Then by the inductive hypothesis $|G/N|$ is divisible by at most 2 primes. If p divides $|G/N|$, then this shows $|G| = p^a q^b$ and we're done. Otherwise N is a Sylow p -subgroup of G and we can assume (for the purpose of contradiction) that $|G| = p^a q^b r^c$ for distinct primes p, q, r . By the Schur-Zassenhaus theorem, let $A \leq G$ be a complement to N , with $|A| = q^b r^c$.

Let $x \in N$ be non-trivial. Suppose $1 \neq a \in A$ centralized x . Then xa would not have prime power order. Thus $C_G(x) \leq N$. By Theorem 6.4, we see that $G = NA$ is a Frobenius group. Let $M \triangleleft A$ be a minimal normal subgroup, with $|M|$ a q -group without loss of generality. Since M is elementary Abelian, by Theorem 6.9 M is of order q . If R is a subgroup of order r in A , then MR has order qr , and again by Theorem 6.9 is cyclic. The generator of MR does not then have prime power order, and this is our final contradiction.

6C

[6C.1]

- (a) If σ has prime order p , then for every $n \neq 0 \pmod{p}$ we have $\langle \sigma^n \rangle = \langle \sigma \rangle$, so that σ^n fixes the same points of G that σ does. That is, σ^n only fixes $1 \in G$. Since this is true for all non-identity elements of $H = \langle \sigma \rangle$, we see that $G \rtimes H$ is a Frobenius group by Theorem 6.4. Thus G is nilpotent by Theorem 6.24.
- (b) Our example comes from finding a subgroup $S \leq \text{SL}(2, \mathbb{F}_5)$ of order 12, acting fixed-point freely on the group $\mathbb{F}_5 \times \mathbb{F}_5$ of order 25. We choose S such that the Sylow 3-subgroup $\langle \phi \rangle = Q \leq S$ is normal and such that the Sylow 2-subgroup $\langle \sigma \rangle = P \leq S$ is cyclic. Now we have the group $G = (\mathbb{F}_5 \times \mathbb{F}_5) \rtimes Q$ is non-nilpotent of order 75, and we will show σ (of order 4) acts fixed-point freely on G .

We let the group H of order 25 be given by $\langle a \rangle \times \langle b \rangle$, with a and b of order 5 each. Then we define $\phi \in \text{Aut}(H)$ (of order 3) as

$$\begin{aligned}\phi(a) &= b^2 \\ \phi(b) &= a^2 b^{-1}\end{aligned}$$

and extend linearly. It's easy to see $|\phi| = 3$ and that it acts non-trivially, so that $\langle \phi \rangle$ is a non-normal Sylow 3-subgroup of $G = H \rtimes \langle \phi \rangle$, so that G is not nilpotent. Finally we define $\sigma \in \text{Aut}(G)$ as

$$\begin{aligned}\sigma(a) &= b \\ \sigma(b) &= a^{-1} \\ \sigma(\phi) &= \phi^{-1}\end{aligned}$$

From the fact $S = \langle \phi, \sigma \rangle \leq \text{SL}(2, \mathbb{F}_5)$ and $Q \triangleleft S$, this does define an automorphism of order 4 of G (it can also be checked directly). We have

$$\sigma(a^r b^s \phi^k) = a^{-s} b^r \phi^{-k}$$

and these are equal only when $r = s = k = 0$, so σ only fixes the identity of G , as desired.

[6C.2]

- (a) A has $p + 1$ subgroups of order p , call them $A_1, \dots, A_{p+1}$. Define $K_i = C_N(A_i)$. Now $K_i > 1$ since otherwise N would be nilpotent by part (a) of the previous problem. Also since $A = \langle A_i, A_j \rangle$ for $i \neq j$, we have

$$K_i \cap K_j = C_N(A_i) \cap C_N(A_j) \leq C_N(A) = \{1\}$$

Since A is Abelian, A_j acts on K_i for $i \neq j$, since we have (with $a_i \in A_i$ and $a_j \in A_j$)

$$(na_j)a_i = n(a_ja_i) = n(a_ia_j) = (na_i)a_j = na_j$$

for all $n \in K_i$ (and thus $na_j \in K_i$). Since $K_i \cap C_N(A_j) = \{1\}$, we see A_j acts fixed-point freely on K_i , so that K_i is nilpotent by part (a) of the previous problem (and the fact $|A_j|$ is prime).

- (b) Since A is a p -group, we have

$$|N| \equiv |C_N(A)| = 1 \pmod{p}$$

and thus we have a coprime action of A on N . By Glauberman's Lemma (in the form of Theorem 3.23), N has an A -invariant Sylow q -subgroup $Q \leq N$. By the same result, any other invariant Sylow q -subgroup of N would be conjugate to Q via an element of $C_N(A) = \{1\}$, and thus Q is the unique A -invariant Sylow q -subgroup of N . Now as above, K_i is A -invariant because A is Abelian, and thus $Q_i \leq K_i$, as a characteristic subgroup, is also A -invariant. So X is an A -invariant q -subgroup of N , whereby Corollary 3.25 $X \leq Q$.

We now give two proofs $X = Q$. The first is easier than the hint in the book. Because A is Abelian and non-cyclic, Theorem 6.21 says

$$Q = \langle C_Q(a) \mid 1 \neq a \in A \rangle$$

But $C_Q(a) = C_Q(A_i)$ for $a \in A_i$, and $C_Q(A_i) = Q \cap K_i = Q_i$. Thus $Q = X$.

The second proof follows the hint, and we assume for the sake of contradiction that $X < Q$. Because X is A -invariant, $N_Q(X)$ is also A -invariant, and normalizers grow in Q . We can thus repeat this process until we find $A \leq Y \triangleleft Q$ with Y a proper normal A -invariant subgroup. By Corollary 3.28 we have (with $Z := Q/Y$)

$$C_Z(A_i) = C_Q(A_i)Y/Y = Q_iY/Y = \{1\}$$

This holds for all $1 \leq i \leq p + 1$, and thus by Theorem 6.4 A acts as a Frobenius complement on Z , which is a contradiction of Corollary 6.10. We've shown then that we must have $X = Q$.

7A

[7A.1] Let G be a simple group, and $M \leq G$ a maximal subgroup that is nilpotent. If p is an odd prime dividing $|M|$, then the Sylow p -subgroup P of M is normal in M . So if $1 < C \leq P$ is characteristic in P , then we have $C \triangleleft M$; since G is simple, this means $M = N_G(C)$. But M of course has a normal p -complement (being nilpotent), so Thompson's theorem implies G has a normal p -complement. This contradicts G being simple, so no odd prime can divide $|M|$, implying M is a 2-group.

[7A.2] If $S := SL(2, 3)$ and $Z \leq S$ is its center, then S/Z has order 12. As shown in the text, S has more than 1 (and hence at least 4) Sylow 3-subgroups. If $P, Q \leq S$ are two of these, then we cannot have $PZ = QZ$, since $|PZ| = |QZ| = 6$ has a unique Sylow 3-subgroup. Thus S/Z has at least 4 Sylow 3-subgroups (meaning it has exactly 4 for cardinality reasons). Counting shows the elements not of order 3 in S/Z form the unique Sylow 2-subgroup, which must be normal. This gives a normal subgroup $K \leq S$ of order 8.

[7A.3]

(a) We have

$$\begin{pmatrix} d_1^{-1} & 0 & \dots & 0 \\ 0 & d_2^{-1} & \dots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \dots & d_n^{-1} \end{pmatrix} \begin{pmatrix} 1 & * & \dots & * \\ 0 & 1 & * & \dots \\ 0 & 0 & \ddots & * \\ 0 & 0 & \dots & 1 \end{pmatrix} \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \dots & d_n \end{pmatrix} = \begin{pmatrix} 1 & * & \dots & * \\ 0 & 1 & * & \dots \\ 0 & 0 & \ddots & * \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

Specifically, if our diagonal matrix X has entries $\{d_1, \dots, d_n\}$ and $A := (a_{ij})$ is any matrix, we have

$$X^{-1}AX = (d_i^{-1}d_j a_{ij})$$

This shows that being upper-triangular ($a_{ij} = 0$ when $i > j$) is preserved by conjugation of $X \in D$, as are any entries on the main diagonal (where $i = j$). Thus $D \leq N_G(P)$.

(b) Since $D \leq N_G(P)$, we know DP is a subgroup. Using the same notation as the previous part, we have

$$XA = (d_i a_{ij})$$

So if A is upper-triangular, so is XA . But we also have

$$\begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \dots & d_n \end{pmatrix} \begin{pmatrix} 1 & * & \dots & * \\ 0 & 1 & * & \dots \\ 0 & 0 & \ddots & * \\ 0 & 0 & \dots & 1 \end{pmatrix} = \begin{pmatrix} d_1 & * & \dots & * \\ 0 & d_2 & * & \dots \\ 0 & 0 & \ddots & * \\ 0 & 0 & \dots & d_n \end{pmatrix}$$

So if A is upper-triangular, we let X be diagonal with entries $\{a_{11}, \dots, a_{nn}\}$, and let $B := (a_{ii}^{-1}a_{ij})$, so that $X \in D$ and $B \in P$ with $XB = A$. This shows DP is exactly the set of upper-triangular matrices.

- (c) Let $\{v_1, \dots, v_n\} \subset V$ be the basis that gives elements of P as upper-triangular matrices. Then the subspace $V_k := \langle v_k, \dots, v_n \rangle$ of V has dimension $n - k + 1$ and is invariant under action by P .

Now let $W \leq V$ be a non-trivial P -invariant subspace, and choose the largest k such that the projection $W \rightarrow \langle v_1, \dots, v_{k-1} \rangle$ has trivial image. This means that for every $w \in W$, if we write it as $w = a_1 v_1 + \dots + a_n v_n$, then $a_i = 0$ for $i < k$. The maximality of k also implies there is some $w_0 \in W$ with $a_k \neq 0$. Define $(b_{ij}) = B \in P$ as

$$b_{ij} = \begin{cases} 0 & i > j \\ 1 & i = j \\ \frac{-a_j}{a_k} & i = k \end{cases}$$

Then it is easy to check that

$$(w_0 B)_j = \sum_i a_i b_{ij} = \begin{cases} 0 & j < k \\ a_k & j = k \\ 0 & j > k \end{cases}$$

Since we assumed W was P -invariant, this implies $a_k v_k \in W$, and so $v_k \in W$. If $(c_{ij}) := C_m \in P$ with $m > k$ is chosen so that it has one off-diagonal 1 at c_{km} , then $v_k C_m = v_k + v_m$. Thus we have that $V_k \leq W$. Because $\dim(W) \leq n - k + 1$ by the projection condition, we must have $W = V_k$. So the V_k are the only P -invariant subspaces of V .

- (d) If $W \leq V$ is P -invariant and $p \in P$ with $n \in N_G(P)$, then for $w \in W$ we have

$$(wn)p = w(np) = w(p'n) = (wp')n \in Wn$$

Thus Wn is a P -invariant subspace, and by the previous part (since $\dim(W) = \dim(Wn)$) we must have $W = Wn$. Since $n \in N_G(P)$ was arbitrary, we have that W is $N_G(P)$ -invariant as well.

Using the basis $\{v_1, \dots, v_n\}$ and the subspaces V_k from the previous part, this shows that every element of $N_G(P)$ is upper-triangular. By parts (a) and (b) then we have $N_G(P) = DP$.

[7A.4] Let $G := GL(2, q)$. From the previous problem, we have that for a Sylow p -subgroup $P \leq G$,

$$|N_G(P)| = |DP| = |D| \cdot |P| = (q-1)^2 q$$

(Note this follows since $D \cap P$ is trivial.) From the formula for $|G|$ we see that $[G : N_G(P)] = q+1$, so G has $q+1$ Sylow p -subgroups.

Let $S = SL(2, q) \triangleleft G$. Because $[G : S] = q-1$ we see that S contains one (hence all) Sylow p -subgroups of G . Thus S has $q+1$ Sylow p -subgroups.

Finally, let $H = PSL(2, q) = S/Z$. If q is even then $H = S$ and we're done. Otherwise if $P, Q \leq S$ are two distinct Sylow p -subgroups, then we cannot have $PZ = QZ$ because $P \triangleleft PZ$ (having index 2), so must be the unique Sylow p -subgroup. Thus the canonical map $S \rightarrow H$ must be injective on the set of Sylow q -subgroups, and we know it is also surjective from [1B.5]. So H has $q + 1$ Sylow p -subgroups as well.

[7A.5] Let $U \triangleleft P$ be elementary Abelian, and choose $E \in \mathcal{E}(P)$ so that $|E \cap U|$ is maximal. We assume $U \not\leq N_P(E)$ and reach a contradiction. Choose $F = E^u \neq E$ for some $u \in U$, and define $H := \langle E, F \rangle$ and $Z := E \cap F$.

First note that Z is centralized by H (since E and F are Abelian), so that $Z(H \cap U)$ is a group. It is Abelian since Z is centralized by the Abelian group $H \cap U$, and it is elementary Abelian since both Z and $H \cap U \leq U$ are.

We have that $UH = UE$, and thus we have

$$\frac{|H|}{|H \cap U|} = \frac{|E|}{|E \cap U|} = \frac{|E|}{|Z \cap U|}$$

where the last equality follows from $E \cap U \leq Z \leq E$, since U is Abelian. From the fact that $|H| \geq |E| \cdot |F|/|Z|$ we then have

$$\begin{aligned} \frac{|E|}{|Z \cap U|} &\geq \frac{|E| \cdot |F|}{|Z| \cdot |H \cap U|} \\ \frac{|Z| \cdot |H \cap U|}{|Z \cap U|} &\geq |F| \end{aligned}$$

Since $Z \cap (H \cap U) = Z \cap U$, the above says that $Z(H \cap U)$ is an elementary Abelian group at least as large as $F \in \mathcal{E}(P)$, so that $Z(H \cap U) \in \mathcal{E}(P)$. But the very first equality above, together with the fact that $|H| > |E|$ (since $E \neq F$) says that

$$E \cap U < H \cap U = (ZU \cap H) \cap U = Z(H \cap U) \cap U$$

And this contradicts the choice of E to maximize $|E \cap U|$. This contradiction shows we must have U normalizing E , as desired.

[7A.6] Let Q be a generalized quaternion group with $|Q| > 8$. If $C \leq Q$ is the cyclic subgroup of index 2, then C is *unique*, because all elements of $Q \setminus C$ have order $4 < |C|$. Thus if $\sigma \in \text{Aut}(Q)$, it restricts to an automorphism of C . So if C is a 2-group, then $\sigma|_C$ has order a power of 2. So for some $k \geq 0$ we have $\phi := \sigma^{2^k}$ acts trivially on C , and then for $g \in Q \setminus C$ we have $\phi(g) = gc^r$, so that $\phi^m(g) = gc^{mr}$, showing that $\phi \in \text{Aut}(Q)$ also has order a power of 2. We have thus shown that if $|Q| = 2^n$ with $n > 3$ then $\text{Aut}(Q)$ is a 2-group.

We know from [3F.3] that $\text{Aut}(Q_8)$ does have an element of order 3. However the same arguments as above show that an element of $\text{Aut}(Q_8)$ fixing a cyclic subgroup of index 2 must have order a power of 2, so that $|\text{Aut}(Q_8)| = 3 \cdot 2^m$.

In the proof of Lemma 7.3, we need to exclude the case that $L \leq SL(2, p)$ is a 2-group. If L is cyclic or quaternion with $|L| > 8$ then $\text{Aut}(L)$ is a 2-group, so P acts trivially. If $L \cong Q_8$ and P does not act trivially, then we need a non-trivial homomorphism $P \rightarrow \text{Aut}(Q_8)$, implying that $p = 3$. So if $p > 3$ then we can remove the Lemma's condition (and the same in Theorem 7.5) that a Sylow 2-subgroup is Abelian.

7B

No problems in this section!

7C

[7C.1] Consider the hypothesis: for a fixed Sylow subgroup $P \leq G$, if $X \leq P$ is characteristic, then $N_G(X)/C_G(X)$ is a p -group. We prove by induction on $|G|$ that such a group has a normal p -complement. So suppose that G satisfies our hypothesis, and all groups of order less than $|G|$ satisfying the hypothesis have a normal p -complement. We work to prove G has a normal p -complement as well.

Let $1 < X \leq P$ be characteristic, for the fixed Sylow subgroup $P \leq G$, and let $H := N_G(X)$. We show that H has a normal p -complement; we write $\bar{Y}$ for subgroups in $\bar{H} := H/X$ via the correspondence theorem. $\bar{P}$ is a Sylow p -subgroup of $\bar{H}$. Also if $\bar{N} \leq \bar{P}$ is characteristic, then $N \leq P$ is characteristic as well, so $N_G(N)/C_G(N)$ is a p -group. Then $N_H(N)/C_H(N)$ is isomorphic to a subgroup of $N_G(N)/C_G(N)$, so is of course also a p -group. But from $X \leq N$ we have $N_{\bar{H}}(\bar{N}) = \overline{N_H(N)}$, and also $\overline{C_H(N)X} \leq C_{\bar{H}}(\bar{N})$. Because we have $X \leq N \leq N_H(N)$, this shows $N_{\bar{H}}(\bar{N})/C_{\bar{H}}(\bar{N})$ is a quotient of $N_H(N)/C_H(N)$, and hence also a p -group. Our hypothesis is then satisfied in $\bar{H}$ with fixed Sylow subgroup $\bar{P}$, and since $|\bar{H}| < |G|$, our induction hypothesis shows $\bar{H}$ has a normal p -complement $\bar{M}$. Note that we have

- $[H : M]$ is a power of p , so that $H = MP$.
- $[M : X]$ is coprime to p , so that $X \triangleleft M$ is a normal Sylow p -subgroup.
- Because $N_M(X)/C_M(X) = M/C_M(X)$ is a p -group, we have $M = XC_M(X)$.

Now $X \cap C_M(X)$ is a central Sylow p -subgroup of $C_M(X)$, so by Burnside's Transfer Theorem, $C_M(X)$ has a normal p -complement Y . Since Y is characteristic in $C_M(X)$ and $C_M(X) = C_H(X) \cap M \triangleleft H$, we have that $Y \triangleleft H$ as well. But

$$[H : Y] = [H : M][M : C_M(X)][C_M(X) : Y]$$

is a power of p , so that Y is a normal p -complement in H , as desired.

We've shown that for any non-trivial characteristic $X \leq P$, $N_G(X)$ has a normal p -complement. In particular, this works for $J(P)$ and $Z(P)$, so by Thompson's theorem G has a normal p -complement, and we're done.

7D

No problems in this section!

8A

[8A.1] Let $|A| = |B| = n$, and consider the right action of A on A , via $x \cdot a = xa$. This is a regular action and embeds A inside S_n . Similarly, we see B embedded in S_n , and both are regular subgroups.

If G is a permutation group with two regular normal subgroups $M, N \triangleleft G$, then for a point stabilizer we must have $G = MG_\alpha = NG_\alpha$ and $M \cap G_\alpha = N \cap G_\alpha = \{1\}$. It is thus enough to find G with a proper subgroup $H < G$ and two normal subgroups with $HN = HM = G$ and $N \cap H = M \cap H = \{1\}$. For this we can take $G = D_8 = \langle (1234), (13) \rangle$, set $M = \langle (1234) \rangle$ to be the rotation subgroup, and $N = \langle (13)(24), (12)(34) \rangle$ to be the reflections not fixing any vertices. Then N and M are both normal in G , and are both complemented by the subgroup $\langle (13) \rangle$. Thus G is a permutation group with two nonisomorphic regular normal subgroups: M is cyclic while N is elementary Abelian (both of order 4).

[8A.2] Suppose $x \in C_G(H)$ fixes a point $\alpha \in \Omega$, on which H acts transitively. For any $\beta \in \Omega$, choose $h \in H$ with $\alpha \cdot h = \beta$. Then

$$\beta \cdot x = \alpha \cdot (hx) = \alpha \cdot (xh) = \alpha \cdot h = \beta$$

And thus x fixes β as well. Since $\beta \in \Omega$ was arbitrary, x acts trivially on Ω , so that $x = 1$. This shows that $C_G(H)$ is semiregular. If H is Abelian, then $H \leq C_G(H)$, so that H is semiregular as well. But H is transitive by hypothesis, so H is regular.

[8A.3] Consider the group $H = G_L \times G_R$, where $G_L \cong G_R \cong G$. Let H act on the set G via

$$g \cdot (a, b) = a^{-1}gb$$

The stabilizer H_1 is precisely the diagonal subgroup, and in general

$$H_g = \{(x, x^g) \mid x \in G\}$$

So if (x, x) fixed every point of G , we would have $x^g = x$ for all $g \in G$, implying $x \in Z(G)$. So when $Z(G) = \{1\}$, the action of H on G is faithful. Both G_L and G_R are normal subgroups of H , and clearly $G_L H_1 = G_R H_1 = H$, with $G_L \cap H_1 = G_R \cap H_1 = \{1\}$. Thus

by Lemma 8.5, G_L and G_R are two distinct regular normal subgroups of the permutation group H , both isomorphic to G .

[8A.4] As in the hint, we assume $G = UV$. Let $K \leq G$ be a point stabilizer. Then $UK = VK = G$ and $U \cap K = V \cap K = \{1\}$. Since $U \cap V = \{1\}$ as well, we see that G is isomorphic to the internal direct product $U \times V$. We thus have

$$U \cong G/V \cong VK/V \cong K/(V \cap K) \cong K \cong K/(U \cap K) \cong UK/U \cong G/U \cong V$$

Now assume $z \in Z(U)$, and choose $k \in K$ mapping to z via the isomorphisms above. Note this implies there's a $v \in V$ with $k = zv$. Since $V \subset C_G(U)$, this implies $k \in C_G(U)$, and by Lemma 8.5 we see that k acts trivially on all points, so that $k = 1$. Thus $Z(U)$ (and hence $Z(V)$) is trivial.

[8A.5] Note that if $x \in N_G(H)$ and $\beta \in \Delta$, then for $h \in H$

$$\beta \cdot x = \beta \cdot (hx) = \beta \cdot (xh^x)$$

and thus $h^x \in H$ fixes $\beta \cdot x$. As h ranges over H , so does h^x , so $\beta \cdot x \in \Delta$, and $N_G(H)$ acts on Δ .

Choose r -tuples $(\beta, \dots)$ and $(\gamma, \dots)$ of distinct elements in Δ . Note that by transitivity, all point stabilizers have the same order, so $H = G_\beta = G_\gamma$. Choose $g \in G$ mapping the first tuple to the second; such a g exists because $r \leq k$. Then

$$H^g = G_\beta^g = G_\gamma = H$$

so $g \in N_G(H)$. Thus $N_G(H)$ acts r -transitively on Δ .

[8A.6] As in the first paragraph of the previous solution (replacing H with P), $N_G(P)$ acts on Δ . For $\beta \in \Delta$, choose $g \in G$ with $\alpha \cdot g = \beta$. Since P fixes β , we have $P \leq G_\beta = H^g$, so that $P^{g^{-1}}$ is a Sylow p -subgroup of H . Choose h in H with $P^h = P^{g^{-1}}$. Then $hg \in N_G(P)$ and

$$\alpha \cdot (hg) = \alpha \cdot g = \beta$$

Since $\beta \in \Delta$ was arbitrary, $N_G(P)$ acts transitively on Δ .

[8A.7] Note that if A has a Frobenius action on N , then by Theorem 6.9 we know A is cyclic. So it is enough to establish the action is Frobenius; we assume the action of A on N is not Frobenius, and reach a contradiction. By Theorem 8.9 we know that N is an elementary Abelian group, and that no nontrivial proper subgroup of N admits an action of A . By assumption there exists $n \in N$ for which $C_A(n) > 1$, and choosing $a \in C_A(n)$, we have $1 < C_N(a) < N$, the second inclusion being proper because A acts faithfully. But for $x \in A$ and $g \in C_N(a)$ we have

$$(g^x)^a = g^{xa} = g^{ax} = (g^a)^x = g^x$$

so that $g^x \in C_N(a)$. This shows $C_N(a)$ is a proper A -invariant subgroup, and this is our contradiction.

[8A.8] Let $\alpha \in \Omega$ and write αN for the N -orbit of α . For $g \in G$ and $n \in N$ we have

$$(\alpha \cdot n) \cdot g = \alpha \cdot (ng) = \alpha \cdot (gn^g) = (\alpha \cdot g) \cdot n^g \in (\alpha \cdot g)N$$

As n ranges over N so does n^g , so we see that $(\alpha N) \cdot g = (\alpha \cdot g)N$, and in particular both orbits have the same size (since g doesn't change subset sizes). If βN is another N -orbit, then choosing $g \in G$ with $\alpha \cdot g = \beta$ shows $(\alpha N) \cdot g = \beta N$, and thus G is transitive on these N -orbits. They then all have the same size, and N is half-transitive.

[8A.9] From the assumption N does not act trivially, choose $\alpha \in \Omega$ so that the N -orbit αN contains $\gamma \neq \alpha$. For $\beta \in \Omega \setminus \{\alpha\}$, choose $g \in G$ with $(\alpha, \gamma) \cdot g = (\alpha, \beta)$. By the previous problem $(\alpha N) \cdot g = \alpha N$, but it also contains $\beta = \gamma \cdot g$. Since β was arbitrary, we see $\Omega \subset \alpha N$, and thus N acts transitively.

Note that the previous problem actually shows the N -orbits are blocks for G , so primitivity implies a non-trivial orbit must be all of Ω . This is proved in two different ways in Lemma 8.15.

[8A.10] Let G be a 4-transitive solvable permutation group. If $N \triangleleft G$ is a minimal normal subgroup, then the previous problem shows N acts transitively, and since N is elementary Abelian [8A.2] shows N acts regularly. Let $H \leq G$ be a point stabilizer, acting 3-transitively on the nontrivial elements of N by Lemmas 8.2 and 8.5. By Lemma 8.8, N is elementary Abelian of order 4. But then G is a permutation group of degree 4, acting 4-transitively, and as shown in the text that implies $G \cong S_4$, since only S_n can act $(n-1)$ -transitively (and faithfully) on n points.

We can also handle the case G is a 3-transitive solvable permutation group. If $V \triangleleft G$ is a minimal normal subgroup, then V is regular, and is an elementary Abelian group. Let H be a point-stabilizer, so that H acts 2-transitively on $V^\#$ (writing $V^\#$ for the nonzero elements). Because H is acting via automorphisms, Lemma 8.8 shows V must either be an elementary Abelian 2-group, of $|V| = 3$. In the case $|V| = 3$, G has degree 3, and so as above we must have $G \cong S_3$. So we consider the case $|V| = 2^n$, and note that $n \geq 2$ since G is 3-transitive. We define $q = 2^n$.

Choose a nonzero element $u \in V$, and let $K \leq H$ be the point stabilizer of u . Since H is solvable, it has a minimal normal subgroup $F \triangleleft H$, which (via [8A.9] and [8A.2]) acts regularly on $V^\#$, so that $|F| = q - 1$. By [8A.7] we must have that F is cyclic. We thus have that $V \cong \mathbb{F}_q^+$, the additive group of the field $\mathbb{F}_q$, and $F \cong \mathbb{F}_q^*$, the multiplicative group of the field $\mathbb{F}_q$. We write u^a for the image of u under the action of $a \in F$. Note that every nonzero vector in V can be written as u^a for a unique $a \in F$ (by regularity).

Define a multiplication on V via $0v = v0 = 0$ and $vu^a = v^a$. Because F is Abelian, this is commutative, and since it's a group action, it is associative and $(u^a)(u^b) = u^{ab}$. Clearly $uu^a = u^a$ and $(u^a)(u^{a^{-1}}) = u$. Because F acts via automorphisms, this multiplication is distributive, and we've made V into the field $\mathbb{F}_q$ with multiplicative identity u .

Now K acts via automorphisms on V , and so preserves the additive structure. We will see that because K normalizes F , it also preserves the multiplicative structure. For $k \in K$ we have

$$(u^a)^k = (u^k)^{a^k} = u^{a^k}$$

because K fixes u . But then

$$(u^a u^b)^k = (u^{ab})^k = u^{(ab)^k} = u^{a^k b^k} = (u^{a^k})(u^{b^k}) = (u^a)^k (u^b)^k$$

and so yes, K preserves the multiplicative structure. Since it preserves the scalars $\{0, u\} \subset V$, K is acting via field automorphisms on V . Note that if $k \in K$ acts trivially on the field V , then it fixes every point of V , and thus k acts trivially; but G is a permutation group, so $k = 1$. In other words, we have an injective map $K \rightarrow \text{Gal}(V/\mathbb{F}_2)$.

But K acts transitively on $V \setminus \{0, u\}$, and so we have

$$2^n - 2 = |V \setminus \{0, u\}| \leq |K| \leq |\text{Gal}(V/\mathbb{F}_2)| = n$$

This implies $n \leq 2$, so we see that $n = 2$ and $|V| = 4$. But then H , acting 2-transitively on $V^\#$, actually acts 3-transitively, and so G is actually 4-transitive, and we've already shown this implies $G \cong S_4$.

[8A.11] Let $T \cong \mathbb{F}_q^+$, the additive group of the field with q elements. Also let $S \cong \mathbb{F}_q^*$, the multiplicative group of the same field. Then $|T| = q$ and $|S| = q - 1$. We let $G := T \rtimes S$ with S acting via scalar multiplication; note that this action is Frobenius, hence (by order considerations) transitive. Since T and S are Abelian, G is solvable. By Lemma 8.6, G acting on the cosets of S is 2-transitive, of degree $[G : S] = |T| = q$. Since $|G| = q(q - 1)$, this must (again by order considerations) be sharply 2-transitive.

[8A.12] G is 2-transitive if and only if the component-wise action on $\Gamma := \{(\alpha, \beta) \mid \alpha \neq \beta \in \Omega\}$ is transitive. Since G acts transitively on the diagonal of $\Omega \times \Omega$ (since it acts transitively on Ω), we see that G is 2-transitive if and only if G has two orbits on $\Omega \times \Omega$. Now $g \in G$ fixes the point $(\alpha, \beta) \in \Omega \times \Omega$ if and only if g fixes both α and β , so that

$$\chi_{\Omega \times \Omega}(g) = \chi_\Omega(g)^2$$

By [1A.6] G has two orbits on $\Omega \times \Omega$ if and only if

$$2 = \frac{1}{|G|} \sum_{g \in G} \chi_{\Omega \times \Omega}(g) = \frac{1}{|G|} \sum_{g \in G} \chi_\Omega(g)^2$$

[8A.13] Throughout we assume $\alpha, \beta, \gamma \in \Omega$ are distinct. G acts 3-transitively if and only if it acts transitively on the set of distinct 3-tuples $\{(\alpha, \beta, \gamma)\} \subset \Omega^3$. Because G acts 2-transitively, it acts transitively on the following disjoint subsets of Ω^3 :

- The diagonal $\{(\alpha, \alpha, \alpha)\}$.
- The three partial diagonals $\{(\alpha, \alpha, \beta)\}$, $\{(\alpha, \beta, \alpha)\}$, and $\{(\beta, \alpha, \alpha)\}$.

Thus G acts transitively on the set of distinct 3-tuples if and only if it has 5 orbits on Ω^3 . Just as in the previous problem, this means G acts 3-transitively if and only if

$$5 = \frac{1}{|G|} \sum_{g \in G} \chi_{\Omega}(g)^3$$

In general, if G acts k -transitively on Ω , then it acts $(k+1)$ -transitively if and only if

$$B_{k+1} = \frac{1}{|G|} \sum_{g \in G} \chi_{\Omega}(g)^{k+1}$$

where B_m is the m th Bell number.

[8A.14] Let $\alpha \in \Omega$ and note that the orbit of H containing α has size $[H : H \cap G_{\alpha}]$. Since $|H \cap G_{\alpha}| \leq |G_{\alpha}|$, we have

$$|\Omega| = [G : G_{\alpha}] \leq [G : H \cap G_{\alpha}] = [G : H][H : H \cap G_{\alpha}]$$

And this shows the H -orbit containing α has size at least $\frac{1}{m}|\Omega|$. Since G acts transitively, all point stabilizers have the same size, and so every H orbit has size at least $\frac{1}{m}|\Omega|$, implying there are at most m orbits.

If $G_{\alpha} \not\leq H$, then $|H \cap G_{\alpha}| \leq \frac{1}{2}|G_{\alpha}|$ since $H \cap G_{\alpha}$ is a proper subgroup of G_{α} . Then the above equation actually reads

$$|\Omega| = [G : G_{\alpha}] \leq \frac{1}{2}[G : H \cap G_{\alpha}] = \frac{1}{2}[G : H][H : H \cap G_{\alpha}]$$

Assuming H contains no point stabilizers, then as above, this means every H -orbit has size at least $\frac{2}{m}|\Omega|$, meaning H has at most $\frac{m}{2}$ orbits.

[8A.15] Assume G acts 2-transitively on the cosets of H . This means the point-stabilizer of the coset H (which is the subgroup H) acts transitively on all other cosets. Thus for $x, y \in G \setminus H$, we have $h \in H$ with $Hxh = Hy$, or equivalently $xhy^{-1} \in H$. But then

$$x \cdot (xhy^{-1}, h) = (xhy^{-1})^{-1}xh = yh^{-1}x^{-1}xh = y$$

Thus $H \times H$ acts transitively on $G \setminus H$. Of course it acts transitively on H , since $1 \cdot (1, h) = h$. So $H \times H$ has two orbits on G .

Conversely, if $H \times H$ has two orbits on G , then one orbit is H (as shown above), implying the other orbit is $G \setminus H$. So for $x, y \in G \setminus H$, there exists $h, k \in H$ with $x \cdot (h, k) = y$, or $h^{-1}xk = y$. But then $y \in Hxk$, showing that $Hxk = Hy$. Since x and y were arbitrary, this shows H acts transitively on the non-trivial cosets of H in G , implying G is 2-transitive on these cosets.

[8A.16] Let $K \leq G$ be a point stabilizer of this action, so that $[G : K] = n$, and let $L \leq K$ be

the stabilizer of a different point in Ω ; since G is 2-transitive, $[K : L] = n - 1$. We will use Lemma 8.5 repeatedly. Because $H \leq G$ is transitive, $HK = G$. Then

$$[K : H \cap K] = [HK : H]$$

is coprime to $n - 1$ (equality follows from Corollary X.11). By Corollary X.12 and Dedekind's Lemma, we have

$$K = L(H \cap K) = HL \cap K$$

Then $K \leq HL$ implies $HL = HK = G$. But L is the point-stabilizer for the component-wise action of G on $\Omega \times \Omega \setminus \Delta$, the distinct tuples of points. So H acts transitively on this set, which is equivalent to H being 2-transitive.

[8A.17] We know $SL(2, q)$ is 2-transitive by Lemma 8.3. If V is our vector space, consider the "horizontal" and "vertical" lines $\{(t, 0) \mid t \in \mathbb{F}_q\}$ and $\{(0, t) \mid t \in \mathbb{F}_q\}$. The stabilizer of both of these lines in $SL(2, q)$ is the diagonal subgroup, which (since determinants are 1) looks like

$$D := \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \mid a \in \mathbb{F}_q^* \right\}$$

All the other lines in V look like $\{(tb, t) \mid t \in \mathbb{F}_q\}$ for nonzero $b \in \mathbb{F}_q$. Now every element has a square root in $\mathbb{F}_q$: this is because q is even, so squaring in the odd-order group $\mathbb{F}_q^*$ is injective, hence surjective. Choose a with $a^2 = b$, and note that

$$(t, t) \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = (ta, ta^{-1})$$

Via the bijection $t \mapsto at$ of $\mathbb{F}_q$, we see that (recalling $a^2 = b$)

$$\{(ta, ta^{-1}) \mid t \in \mathbb{F}_q\} = \{(tb, t) \mid t \in \mathbb{F}_q\}$$

So D acts transitively on these $q - 1$ lines. Since $|D| = q - 1$, it is acting regularly, and $SL(2, q)$ is then sharply 3-transitive.

8B

[8B.1] Consider $G \leq S_\Omega$ and let $U \subset G$ be those elements whose translates of X contain the element α :

$$U := \{g \in G \mid \alpha \in Xg\}$$

This means that

$$\Delta = \bigcap_{u \in U} Xu$$

Thinking of $G \leq S_G$ acting on itself via right multiplication, define $K := G_{(U)}$, the setwise stabilizer of the subset U . We will show that $\Delta = \alpha K$, and that $G_\alpha \leq K$, so that Δ is a block via Lemma 8.13.

Writing $H := G_\alpha$, note that if $u \in U$ and $h \in H$, then $\alpha \in Xu$, and hence $\alpha = \alpha \cdot h \in Xu h$. This means $uh \in U$; since $u \in U$ was arbitrary, we see that $h \in K$; since $h \in H$ was arbitrary, we see $H \leq K$.

Now let $k \in K$. By definition of K , we have

$$\alpha \cdot k \in \bigcap_{u \in U} Xuk = \bigcap_{u \in U} Xu = \Delta$$

Thus $\alpha K \subset \Delta$. But if $\beta \in \Delta$, choose $g \in G$ with $\alpha g = \beta$. Then for $u \in U$, we see that $\beta \in Xu$ implies $\alpha \in Xug^{-1}$, so that by definition $ug^{-1} \in U$. This shows that g^{-1} (and hence g) setwise stabilizes U , and thus $g \in K$. We then have the reverse containment $\Delta \subset \alpha K$, and we're done.

[8B.2] Suppose no such element $g \in G$ existed. Then whenever $\alpha \in Xg^{-1}$, we also have $\beta \in Xg^{-1}$. If we define Δ as in the previous problem, we then have

$$\{\alpha, \beta\} \subset \Delta \subset X$$

and Δ is a block. It is then a non-trivial block, contradicting that G acts primitively. This contradiction establishes there must be $g \in G$ with $\alpha g \in X$ but $\beta g \notin X$.

[8B.3] Note that $M \cap N = \{1\}$ by minimality. By Lemma 8.15, M and N are transitive. Then by [8A.2], $C_G(M)$ acts semiregularly. But $N \leq C_G(M)$, so that N acts regularly, and $C_G(M)$ is also regular (because we now know it's transitive). Then $|N| = |C_G(M)|$, implying $N = C_G(M)$. Similar reasoning shows $M = C_G(N)$ is regular, and we've established (a) and (b). Part (c) follows from an application of [8A.4] since $M \cap N = \{1\}$.

[8B.4] Let $N, K \triangleleft G$ be distinct minimal normal subgroups of G . By part (b) of the previous problem, $K = C_G(N)$. But G is solvable, so N is Abelian, implying $N \leq C_G(N)$. Minimality then forces $K = N$, a contradiction. Thus G has a unique minimal normal subgroup N . Also we know N is Abelian, hence regular by [8A.4]; because it is elementary Abelian, $|N| = p^k$ for some prime p and integer k , and thus the degree of G is p^k , as desired.

[8B.5] Suppose H fixes the point $\beta \neq \alpha$, and choose $g \in G$ such that $\alpha \cdot g = \beta$. Since $H^g = G_\beta$ has the same order as H , saying that $H \subset H^g$ just implies $H = H^g$. In other words, g normalizes H . But H is maximal (since G is primitive), and $g \notin H$ since it doesn't fix α , so we see that $H \triangleleft G$. But G is faithful, so H must be core-free: we have shown $H = \{1\}$. Since H is maximal, G has no proper non-trivial subgroups, so it is cyclic of prime order.

[8B.6] Note that H cannot fix a point in $\Omega \setminus \{\alpha\}$, since then H fixes every point by the previous problem, so can't have an orbit of size 2. Let $\{\beta, \gamma\}$ be the orbit of H , and define $D := H_\beta$, so that $[H : D] = 2$ and $D \triangleleft H$. Choose $g \in G$ with $\alpha \cdot g = \beta$, and note $D \leq H^g$. But $|H| = |H^g|$ so we have $[H^g : D] = 2$ and $D \triangleleft H^g$. Since H is maximal and $H^g \neq H$, we have

$$N_G(D) \geq \langle H, H^g \rangle = G$$

Since H is core-free however (as G is faithful), this implies $D = \{1\}$, so that $|H| = 2$. Thus $\langle H, H^g \rangle = G$ shows G is generated by two involutions, so as shown before we have a dihedral group: $G \cong D_{2m}$ for some integer $m > 1$ (the $m = 1$ case implies H is trivial, which we've ruled out).

If $C_m \triangleleft D_{2m} \cong G$ is the group of rotations, then every proper subgroup $K \leq C_m$ is normal in G , and thus $KH < G$ is a proper subgroup containing H . But H is maximal because G is primitive, so C_m can have no proper non-trivial subgroups: $m = p$ is a prime. Note that G cannot be Abelian (since it is transitive but not regular), so we must have $p > 2$.

[8B.7] Let $\{\beta, \gamma, \delta\}$ be the orbit of size 3 for $H := G_\alpha$, and let $D := H_\beta$. Then $[H : D] = 3$ and we will be done if we can show D is a 2-group; equivalently, if we can show $O^2(D) = \{1\}$. We do this as in the previous problems: we show $O^2(D) \triangleleft G$, and since G is faithful, H is core-free, so we will be done.

Let $K \triangleleft H$ be the core of D in H ; it is the kernel of the map from H to the symmetric group on $\{\beta, \gamma, \delta\}$. Now $[H : D]$ divides $[H : K] \leq 3!$, so we have $[H : K]$ is either 3 or 6; this implies $[D : K] \leq 2$. Then $O^2(K)$ is characteristic in K , hence normal in D , and

$$[D : O^2(K)] = [D : K][K : O^2(K)]$$

is a power of 2. This implies $O^2(D) \leq O^2(K)$. However $O^2(D) \triangleleft K$ (since $K \leq D$) and $K/O^2(D)$ is a subgroup of the 2-group $D/O^2(D)$. This implies the reverse containment $O^2(K) \leq O^2(D)$, so that $O^2(D) = O^2(K)$. Of course $O^2(K) \triangleleft H$, so we have shown H normalizes $O^2(D)$.

Note that none of the above relied on the permutation action on Ω ; once we knew the finite group H had a subgroup of index 3, by looking at the action on right cosets, we deduced $O^2(D) \triangleleft H$. Choosing $g \in G$ with $\alpha \cdot g = \beta$, we have $D \leq H^g$, and the same argument (since $[H^g : D] = 3$) shows $O^2(D) \triangleleft H^g$. Thus

$$N_G(O^2(D)) \geq \langle H, H^g \rangle = G$$

and we're done.

[8B.8] Let Δ be a block for G , and assume $|\Delta| > 1$; it is enough to show $\Delta = \{1, 2, \dots, n\}$. First we show that some translate of Δ contains elements i, j with $i \leq m$ and $j > m$. If this is not already the case, then either $\Delta \subset \{1, \dots, m\}$ or $\Delta \subset \{m+1, \dots, n\}$. In the former case, let $\alpha \in \Delta$ be the largest element; then $m+1 \in \Delta x^{m-\alpha+1}$, and all other elements of this translate are at most m . In the latter case, let $\alpha \in \Delta$ be the smallest element; then $m \in \Delta x^{m-\alpha}$, and all other elements of this translate are larger than m . Thus we always have a translate Δg , with $g \in G$, such that the elements $i, j \in \Delta g$ exist. Because Δg is also a block, and it is enough to show $\Delta g = \{1, 2, \dots, n\}$, we assume throughout the rest of the solution that $i, j \in \Delta$.

By the transitivity of H , for any $1 \leq k \leq m$, we have $h \in H$ with $i \cdot h = k$. Since $j \cdot h = j$, we have

$$j \in \Delta \cap \Delta h$$

Since Δ is a block, we have $\Delta h = \Delta$, so $k \in \Delta$. We have shown then that $\{1, \dots, m\} \subset \Delta$. Let $1 \leq r \leq n$ be the smallest integer not contained in Δ , and we finish by showing such an r cannot exist by contradiction. We know $r > m$ and $(r-1) \in \Delta$. If $h \in H$ is such that $2 \cdot h = 1$, then

$$1 \in \Delta \cap \Delta(xh)$$

Hence $\Delta(xh) = \Delta$, so that $r = (r-1) \cdot (xh) \in \Delta$, and that is our contradiction.

[8B.9] Note that for $1 < i < m$ we have $i \cdot x = i \cdot y$ and similarly $i \cdot x^{-1} = i \cdot y^{-1}$. And of course y acts trivially on $j > m$. We then compute directly

$$i \cdot (y^{-1}xyx^{-1}) = \begin{cases} i & 1 < i < m \\ i & m < i < n \\ m & i = 1 \\ n & i = m \\ 1 & i = n \end{cases}$$

Thus $(y^{-1}xyx^{-1})$ acts as the 3-cycle $(1, m, n)$. By Corollary 8.19 and the previous problem (with $H = \langle y \rangle$) we know that G is either A_n or S_n . Since A_n consists of all even permutations, $G \leq A_n$ if and only if both generators x and y are even permutations, which is the case precisely when m and n are both odd.

[8B.10] We know $|G| = (n-1)!$. Let the largest orbit $O \subset \{1, \dots, n\}$ of G have size r , noting that $r > 1$ since G is faithful. Then $G \subset S_{(O)}$, which has size $r!(n-r)!$. We then compute

$$\begin{aligned} n|G| &\leq n(r!(n-r)!) \\ \binom{n}{r} &\leq n \end{aligned}$$

This is only possible if $r \geq n-1$. But if $|O| = n-1$ then G lives in the point stabilizer S_α with $\alpha = \{1, \dots, n\} \setminus O$. Since $|G| = |S_\alpha|$ we would have that $G = S_\alpha$ is a point stabilizer, which we assumed is not true. Thus $r = n$ and G is transitive.

Now $[S_n : G] = n$ is coprime to $n-1$, so [8A.16] shows G is 2-transitive, hence primitive. Bochert's theorem then says

$$n = [S_n : G] \geq [(n+1)/2]!$$

It's easy to see this holds true for $\{1, 2, 3, 4, 6\}$. When $n \geq 7$, let $k = [(n+1)/2]$ so that $n \leq 2k$ and $k \geq 4$. So

$$n \leq 2k < 3k \leq k(k-1) \leq k!$$

And thus only $\{1, 2, 3, 4, 6\}$ satisfies this inequality. Direct checks show the subgroup G cannot exist in S_n for $n \leq 4$. But if S_5 acts on its 6 Sylow 5-subgroups, the core is trivial: in section 8C it's proved that $A_6 \triangleleft S_6$ is the only proper nontrivial normal subgroup. This action gives an embedding of S_5 into S_6 as a transitive subgroup. So we've shown $n = 6$ is the only case where this happens.

8C

[8C.1] Suppose $H \leq A_6$ has order 120. Then A_6 acting on the cosets of H induces a homomorphism from A_6 to a transitive subgroup of S_3 ; the kernel K of this homomorphism is such that $3 \leq [A_6 : K] \leq 6$. Thus K is a non-trivial normal subgroup of A_6 , contradicting its simplicity. Thus H doesn't exist.

If G was a simple group of order 120, it would need to have 6 Sylow 5-subgroups. G acting via conjugation on these would give a homomorphism $\phi : G/O_5(G) \rightarrow S_6$. But G is simple, so $O_5(G) = \{1\}$ and the image lands in A_6 (since otherwise $A_6 \cap \phi(G)$ would be a nontrivial normal subgroup of $\phi(G) \cong G$). But then $\phi(G)$ is a subgroup of order 120 in A_6 , which we just showed can't exist. Thus G doesn't exist either.

[8C.2] Let $P \leq G$ be a Sylow 11-subgroup. Then by the orbit-stabilizer theorem (and the fact P only has two subgroups), we see P acts trivially or transitively. The former case is ruled out because G is faithful, and thus P (hence G) is transitive. Since G has prime degree, it is primitive. We let $H \leq G$ be a point stabilizer for $\alpha \in \Omega$, so that $[G : H] = 11$ and H is a maximal subgroup.

First, consider an element $z \in H \cap C_G(P)$. If $1 \neq x \in P$, we have

$$(\alpha \cdot x) \cdot z = (\alpha \cdot z) \cdot x = \alpha \cdot x$$

Thus z fixes the entire orbit of x , which is the entire orbit of P , which is all of Ω . Thus z acts trivially, and $z = 1$. We have then shown $C_G(P) \cap H = \{1\}$. We then have

$$720 \cdot 11 = |G| \geq |C_G(P)H| = |C_G(P)| \cdot |H| = 720|C_G(P)|$$

so that $C_G(P) = P$. Note that $N_G(P)/C_G(P)$ embeds in $\text{Aut}(P)$, of order 10, so that $[N_G(P) : P]$ divides 10. Since then $|N_G(P)| \leq 110$ and $[G : N_G(P)] \equiv 1 \pmod{11}$, the only possibility is $N_G(P)$ has order 55.

Now suppose $1 < N \triangleleft G$ is a minimal normal subgroup; we show $N = G$ to conclude G is simple. By Lemma 8.15, N is transitive, so that 11 divides $|N|$ and thus $P \leq N$. Frattini's argument shows $G = N_G(P)N$, and order considerations then show $G = N$ or $[G : N] = 5$. We can rule the latter case out as follows: $N_N(P) = N_G(P) \cap N = P$, and by Burnside's transfer theorem N has a normal p -complement, which is then normal in G , contradicting the minimality of N . So we've shown $N = G$ and thus G is simple.

[8C.3] Let H be the stabilizer of $\alpha \in \Omega$, and note that H acting on $\Omega \setminus \{\alpha\}$ satisfies the hypotheses of the previous problem, so that H is simple and is transitive on $\Omega \setminus \{\alpha\}$. Thus G is 2-transitive and hence primitive. If $1 < N \triangleleft G$ is a minimal normal subgroup, primitivity implies it is transitive so that $G = NH$. However, $N \cap H \triangleleft H$, so by simplicity we have either $N \cap H = \{1\}$ or $N \cap H = H$. The latter case implies $G = NH = N$, so we show the former case cannot happen to conclude G is simple.

If $N \cap H = \{1\}$, then N is a regular normal subgroup, so that $|N| = 12$. But a group of order 12 has a normal Sylow subgroup (Theorem 1.31), which is then normal in G ; this contradicts the minimality of N , so such an N cannot exist, and we're done.

[8C.4] Let Δ be a block for G that contains α . Write $H := G_\alpha$. For any $h \in H$ we have

$$\alpha \in \Delta \cap \Delta h$$

and thus, being a block, we have $\Delta h = \Delta$. Since H fixes Δ setwise, we know Δ is a union of orbits of H . Then $|\Delta|$ is a sum of these orbit sizes, and divides $|\Omega| = 100$; the only possibilities are $|\Delta| = 1$ or $|\Delta| = 100$. Thus G only has nontrivial blocks, and must be primitive.

Now let $1 < N \triangleleft G$ be a minimal normal subgroup, which is then transitive so that $G = NH$. Since H is simple, as in the previous problem we have $N \cap H = H$ (and thus $N = G$) or $N \cap H = \{1\}$, and N is regular. But this latter case can't happen, since then $|N| = 100$, and a Sylow 5-subgroup P would be normal in N , hence also in G , contradicting minimality. So the only case that happens is $N = G$, and we've shown G is simple.

[8C.5] This problem is not correct as stated: the setwise stabilizer of 3 points has a normal subgroup (of index $3! = 6$) given by the pointwise stabilizer of those 3 points. We instead correct the hypothesis to be: the pointwise stabilizer L of 3 points $\{\alpha, \beta, \gamma\}$ is simple.

Let K be the pointwise stabilizer of $\{\alpha, \beta\}$, so that $L \leq K$ and K is 3-transitive on $\Omega \setminus \{\alpha, \beta\}$. Let $1 < N \triangleleft K$ be a minimal normal subgroup, which is transitive and hence $K = NL$. Simplicity implies $N \cap L = L$ (and then $K = N$) or $N \cap L = \{1\}$ (and N is a regular normal subgroup). We show the latter case can't happen to conclude K is simple. But a group of order $|N| = 22$ has a normal Sylow 11-subgroup, which would then be normal in K , contradicting minimality. So K is indeed simple.

Let H be the stabilizer of α , so that $K \leq H$ and H is 4-transitive. Let $1 < N \triangleleft H$ be a minimal normal subgroup; then as above either $N = H$ or $N \cap K = \{1\}$ and N is a regular normal subgroup. But then K acts 3-transitively via conjugation on $N \setminus \{1\}$, and Lemma 8.8 then shows $|N| = 4$, which contradicts $|N| = 23$. So we must have $N = H$ and H is also simple.

Finally let $1 < N \triangleleft G$ be a minimal normal subgroup, and as above we show the case N a regular normal subgroup gives a contradiction. But H would then be acting 4-transitively

via automorphisms on $N \setminus \{1\}$, which by Lemma 8.8 cannot happen. So G is, yet again, simple.

[8C.6] The problem is not correct as stated. We restrict attention to finite Abelian groups (note $\text{Aut}(\mathbb{Z}) \cong C_2$ is simple), and instead show: A is cyclic of order $\{3, 4, 6\}$, or A is an elementary Abelian 2-group of order at least 8. We will need the following easy fact: let $K \leq Z(G)$ for G a finite group, and suppose we have a homomorphism $\phi : G/K \rightarrow K$. Then the map $\psi : G \rightarrow G$ given by $\psi(g) = g\phi(\bar{g})$ is an automorphism. To see this, we use the fact K is central:

$$\psi(gh) = gh\phi(\overline{gh}) = gh\phi(\bar{g})\phi(\bar{h}) = g\phi(\bar{g})h\phi(\bar{h}) = \psi(g)\psi(h)$$

Also, if $g\phi(\bar{g}) = 1$, then $g = \phi(\bar{g})^{-1} \in K$, so that $\bar{g} = 1$, and thus $g = \psi(g) = 1$. This shows ψ is injective, and since G is finite, it is also surjective. Thus ψ is indeed an automorphism of G , as claimed.

Let ι be the inversion automorphism on A . Then for $\phi \in \text{Aut}(A)$ we have

$$\phi\iota(a) = \phi(a^{-1}) = \phi(a)^{-1} = \iota\phi(a)$$

Thus ι is central in $\text{Aut}(A)$. Since $\text{Aut}(A)$ is simple, this means either (i) ι is trivial, or (ii) $\text{Aut}(A) = \langle \iota \rangle = \{1, \iota\}$. In case (i), every element is its own inverse, so A is an elementary Abelian 2-group, and $\text{Aut}(A) \cong GL(n, 2) \cong SL(n, 2) \cong PSL(n, 2)$. This is trivial when $n = 1$, is non-simple ($\cong S_3$) when $n = 2$, and is simple when $n \geq 3$. Thus in case (i) $\text{Aut}(A)$ is simple precisely when A is elementary Abelian of order at least 8, so we can focus on the case (ii) for the rest of the solution.

If A is non-cyclic, it can be written as $A \cong B \times C$ with B cyclic and some prime p dividing both $|B|$ and $|C|$. Let $B = \langle b \rangle$ and let $x \in C$ have order p . Then the map $b \mapsto x$ defines a homomorphism $\phi : B \rightarrow C$, and as above it lifts to an automorphism ψ of A . Note that $\psi(b) = bx \notin B$, so $\psi \in \text{Aut}(A) \setminus \{1, \iota\}$, and that is a contradiction. Thus A must be cyclic. Since then we have $2 = |\text{Aut}(A)| = \phi(|A|)$, we see that A must have order in $\{3, 4, 6\}$.

8D

[8D.1] Suppose $m_2 = 2$. As shown in [8B.6], a point stabilizer G_α would have order 2. Since it fixes no other point of Ω besides α , all of its orbits on Ω must have size 2, so that $m_i = 2$ for $i > 1$.

[8D.2] Let $\{m_1, \dots, m_r\}$ the subdegrees for G , noting that $\sum m_i = 8$. If $m_2 = 2$ then $m_i = 2$ for all $i > 1$ by the previous problem, so that

$$8 = \sum_{i=1}^r m_i = 1 + \sum_{i>1}^r m_i = 1 + 2(r-1)$$

This represents 8 as an odd number, which is ridiculous, so $m_2 > 2$. The only possible partitions of the number 8 then are $\{1, 3, 4\}$ and $\{1, 7\}$. The first case cannot happen because $3 > 1$ is coprime to the largest subdegree 4, contradicting Theorem 8.38. So we must have subdegrees $\{1, 7\}$, showing that G has rank 2 and is thus 2-transitive.

[8D.3] Let $\{m_1, \dots, m_r\}$ be the subdegrees of G . Then

$$|\Omega| = \sum_{i=1}^r m_i \leq 1 + (r-1)n$$

Letting $m = 1 + (r-1)n$, we then see that G embeds in S_Ω , which is naturally a subgroup of S_m , so that $|G| \leq m!$.

[8D.4] Let $\alpha \in \Omega$ and write $K := K_m(\alpha)$ for the subgroup of G .

- (a) We know $k_1 = 1$ when $m = 1$, so we consider the case $m > 1$. Let $\Delta(\alpha)$ be the orbit of G_α with size m , and let $\beta \in \Delta(\alpha)$ be distinct from α ; note that $G_\beta \leq K$ by definition. Then we have

$$k_m = \frac{|K|}{|G_\alpha|} \geq \frac{|G_\alpha G_\beta|}{|G_\alpha|} = \frac{|G_\beta|}{|G_\alpha \cap G_\beta|} = [G_\beta : G_\alpha \cap G_\beta] = [G_\alpha : G_\alpha \cap G_\beta] = m$$

Where we've used that $|G_\beta| = |G_\alpha|$.

- (b) If $k_m = m$, then we have equality in the above equation, so that $|K| = |G_\alpha G_\beta|$, and thus $K = G_\alpha G_\beta$ is a subgroup of G . Note that this works for any orbital Δ with subdegree m , and any $\beta \in \Delta(\alpha)$, so this holds true for all m -arrows $\alpha \rightarrow \beta$.
- (c) Note that $m > 1$ implies G is non-trivial. Suppose that $k_m \leq m$, and we reach a contradiction. By the above, we must have $k_m = m$ and that $G_\alpha G_\beta$ is a subgroup for an m -arrow $\alpha \rightarrow \beta$. But $m > 1$ implies $\beta \neq \alpha$ and G acting primitively implies G_α is maximal, so $G_\alpha < G_\alpha G_\beta \leq G$ means $G = G_\alpha G_\beta$. However G_β is conjugate to G_α because G is transitive, so that by [1A.4] we have $G = G_\alpha$, giving the contradiction that $G = \{1\}$. We've thus shown that $k_m > m$.

[8D.5] By Theorem 8.42 we have that k_m divides n ; we complete the solution by showing $k_m = m + 1$. But $k_m = [K_m(\alpha) : G_\alpha]$ divides $1 + m + n = |\Omega| = [G : G_\alpha]$, implying that k_m divides $|\Omega| - n = m + 1$. By the previous problem $k_m \geq m > 1$, and thus the only way to divide $m + 1$ is if $k_m = m + 1$.

[8D.6] First let's show the hint: let $X \leq Y$ be finite groups with $[Y : X] = p$ a prime number. The action of Y on the cosets of X gives a map $Y \rightarrow S_p$; let K be the kernel of this action, the core of X . Then $[X : K]$ divides $(p-1)!$, so is coprime to p . This means $O^{p'}(X) \leq K$, and hence $O^{p'}(K) \leq O^{p'}(X)$. But $O^{p'}(K)$ is characteristic in K , hence normal in X (and also in Y), and $[X : O^{p'}(K)]$ is coprime to p , meaning $O^{p'}(X) \leq O^{p'}(K)$, and we have equality: $O^{p'}(X) = O^{p'}(K)$, and the latter we've already said is normal in Y .

Now let G act primitively on Ω and let $\alpha \in \Omega$. Since p is a subdegree, let $\beta \neq \alpha$ be an element in an orbit of size p of G_α . The orbit-stabilizer theorem then shows that this is equivalent to $[G_\alpha : G_\alpha \cap G_\beta] = p$. Writing $L := O^{p'}(G_\alpha \cap G_\beta)$, the previous paragraph shows $L \triangleleft G_\alpha$. Similarly, $[G_\beta : G_\alpha \cap G_\beta] = p$ since $|G_\alpha| = |G_\beta|$, and thus by the previous paragraph again $L \triangleleft G_\beta$. But $G_\alpha \neq G_\beta$ and G_α is maximal in G by primitivity, so L is normal in $\langle G_\alpha, G_\beta \rangle = G$. But G_α is core-free since G is faithful, and hence $L = \{1\}$. By the definition of L , this shows $G_\alpha \cap G_\beta$ is a p' -group, so that $|G_\alpha|$ is only divisible by p , not p^2 . Since subdegrees are indices of subgroups of G_α , they must divide $|G_\alpha|$, and hence p^2 divides no subdegree.

9A

[9A.1] First note that if $E(X) \leq Y \leq X$, then every component of X is a component of Y , so that $E(X) \leq E(Y)$. If in addition Y is normal in X , then every subnormal subgroup of Y is subnormal in X , so that every component of Y is a component of X , and we thus have equality: $E(Y) = E(X)$.

Now if $C \leq H$ is a component of H , then $[C, F(G)] \leq [E(H), F(G)] = 1$, where the last equality follows from $F(G)$ being a normal solvable subgroup. If $C \not\leq E(G)$, then every component $D \leq E(G)$ is also a component of H distinct from C , so $[C, D] = 1$ as well. Thus if $C \not\leq E(G)$, then C centralizes $E(G)$ as well, so $C \leq C_H(F^*(G)) \leq C_G(F^*(G)) \leq F^*(G)$. Thus in all cases $C \leq F^*(G)$. We thus have $E(H) \leq F^*(G)$. Since $F^*(G)$ is normal in both H and G , as shown in the first paragraph we then have

$$E(H) = E(F^*(G)) = E(G)$$

[9A.2] Let $S \triangleleft G$ be the socle, and let $\mathcal{A}$ be the Abelian minimal normal subgroups of G , and $\mathcal{N}$ the non-Abelian ones. Write $X = Z(S)$, and note that for $A \in \mathcal{A}$, we have that A is centralized by all elements of $\mathcal{A}$ and $\mathcal{N}$, so that $A \leq X$.

We also define $Y := \prod_{N \in \mathcal{N}} N$. Each $N \in \mathcal{N}$ is semisimple, so is a product of normal non-Abelian simple subgroups. For $M \neq N$ in $\mathcal{N}$, we have that M centralizes N , hence normalizes these non-Abelian simple subgroups. In other words, the minimal normal subgroups of N are normal in Y . Since N was arbitrary, this shows Y is a product of normal non-Abelian simple subgroups. Then Y is semisimple and normal in S as a direct product of normal subgroups. We have $X \cap Y \leq Z(Y) = \{1\}$, and also that $S = XY$, as the product of all minimal normal subgroups. Hence $S \cong X \times Y$.

[9A.3] Since G is semisimple, it is the direct product of its minimal normal subgroups, all of which are non-Abelian simple. Let $\mathcal{U}$ be those minimal normal subgroups contained in N , and $\mathcal{V}$ those that are not. We define U and V as products over $\mathcal{U}$ and $\mathcal{V}$, respectively, so that $G = U \times V$. For every $M \in \mathcal{V}$, we have $N \cap M \triangleleft M$, so that $[N, M] \leq N \cap M = \{1\}$.

Thus N centralizes V , and $N \cap V \leq Z(V) = 1$. Because $U \leq N$, we have by Dedekind's Lemma

$$U = U(V \cap N) = UV \cap N = G \cap N = N$$

Thus N is the product of the minimal normal subgroups it contains.

[9A.4] First define $Z := Z(E)$ and suppose $C \leq NZ$ is a component of G . If $N \cap C \neq C$, then $C/(N \cap C)$ is a quasisimple group isomorphic to a subgroup of the Abelian group NZ/N , which is a contradiction. Thus $N \cap C = N$ and C is a component of G contained in N .

Now let M be the product of all the components of G contained in N . Using overbar to denote images in E/Z , we have that $\overline{N} \triangleleft \overline{E}$, which is a semisimple group. By the previous exercise, $\overline{N}$ is the product of all the minimal normal subgroups of $\overline{E}$ that it contains. The minimal normal subgroups of $\overline{E}$ are precisely the $\overline{C}$ for components C of G . Thus $\overline{N}$ is the product of components $\overline{C}$ for which $C \leq NZ$; by the first paragraph, these are components contained in N , so that $\overline{N} = \overline{M}$. Thus $N \leq MZ$, and Dedekind's Lemma gives

$$N = MZ \cap N = M(Z \cap N)$$

[9A.5] Let $E := E(G)$. Then $H \cap E \triangleleft E$, and by the previous exercise we can write $H \cap E = MY$, where M is the product of all components contained in $H \cap E$, and $Y = H \cap Z(E)$. Now Y centralizes C , and since C is not contained in $H \cap E \leq H$, M also centralizes C , so that

$$[H \cap E, C] = [MY, C] = \{1\}$$

But $[H, C] \leq [H, E] \leq H \cap E$, so that $[C, H, C] = [H, C, C] = \{1\}$. By the Three Subgroups Lemma, we have

$$[C, H] = [C, C, H] = \{1\}$$

using the fact that C is perfect.

[9A.6] Suppose C is a component of G not contained in H . By the previous exercise, $[C, H] = 1$ and thus $C \leq C_G(H) \leq H$, a contradiction. So every component of G is contained in H , meaning $E(G) \leq H$.

[9A.7] First note that the $\mathcal{X}$ are precisely the minimal normal subgroups of N . Since G is acting via automorphisms, it certainly preserves the set of minimal normal subgroups, so G does indeed act on $\mathcal{X}$. Suppose $\mathcal{Y} \subset \mathcal{X}$ is an orbit of G acting via conjugation. Then if we define

$$M = \prod_{K \in \mathcal{Y}} K$$

we have that $M \triangleleft N$ is preserved by the action of G , so that $M \triangleleft G$. Since N is a minimal normal subgroup of G , we must have $M = N$. Note that, as mentioned in the problem, both N and M are direct products of $\mathcal{X}$ and $\mathcal{Y}$, respectively. Since all elements of $\mathcal{X}$ have non-trivial order, and $|M| = |N|$, it must be that $\mathcal{Y} = \mathcal{X}$, and G acts transitively.

[9A.8] First consider the case G is Abelian. If the prime p divides $|G|$, then a Sylow p -subgroup of G is characteristic, so G is a p -group. Then $\Phi(G) < G$ is characteristic, hence trivial. This shows G is an elementary Abelian p -group, so a direct product of cyclic groups of order p . Thus the problem statement holds true when G is Abelian.

Now suppose G is non-Abelian. Let $H := G \rtimes \text{Aut}(G)$. If $N \leq G$ is normal in H , then it is invariant under the action of $\text{Aut}(G)$, and hence is characteristic. This implies $N = \{1\}$ or $N = G$, so G is a non-Abelian minimal normal subgroup of H . G is semisimple, and so is a direct product over $\mathcal{X}$, its set of minimal normal subgroups, all of which are non-Abelian simple. By the previous problem, H acts transitively on $\mathcal{X}$ via conjugation, and thus every element of $\mathcal{X}$ is isomorphic.

9B

[9B.1] Let $T := C_G(S)$. Note that $T \cap S \leq Z(S) = 1$. If $g \in G$, then it induces an automorphism of $S \triangleleft G$, so by completeness there exists $s \in S$ acting the same way. Then $s^{-1}g \in T$, and thus $g \in ST$. We've thus shown $G = S \times T$.

[9B.2] Suppose $G \triangleleft G_i$ for $i > 1$. Then for $\alpha \in G_i$, conjugation by α would induce an automorphism of G . Thus there is an element $\beta \in G_2$ acting the same way, so that $\alpha^{-1}\beta$ centralizes G . By Lemma 9.12, this implies $\alpha = \beta \in G_2$, so that $G_i = G_2$. Note this problem can be rephrased as: if G is centerless and characteristic in $\text{Aut}(G)$, then $\text{Aut}(G)$ is complete.

[9B.3] We will apply the previous problem, and to do so we need to show that $Z(G) = 1$ and that G is characteristic in $A := \text{Aut}(G)$. G is the direct product of non-Abelian simple groups, so of course $Z(G) = 1$. Let $N \triangleleft G$ be a minimal normal subgroup of G , so it is non-Abelian simple. Then N is subnormal in A , and by Lemma 9.17 we see that N^A is a minimal normal subgroup of A , and N is contained in the socle of A . Since G is the direct product of its minimal normal subgroups, we have G contained in the socle of A . If $M \triangleleft A$ was a minimal normal subgroup not contained in G , then it would commute with $N^A \leq G$ for all such minimal normal subgroups $N \leq G$, implying that M centralized G . But $C_A(G) = \{1\}$ by Lemma 9.11(c), and this contradicts M being non-trivial. So we see that all minimal normal subgroups of A are contained in G , and hence G is the socle of A . This is clearly characteristic, so we're done.

[9B.4] Let D be the dihedral group of order $2n$, with n odd, and $C \triangleleft D$ the cyclic subgroup generated by c . Note that $C = D'$ so that C is characteristic in D . If $\iota \in D \setminus C$ is an involution, then $c^\iota = c^{-1} \neq c$ (because n is odd), so $C \cap Z(D) = \{1\}$. Since ι could be any element of $D \setminus C$, we see that no involutions are in $Z(D)$, so it is trivial. Thus we can consider D as a normal subgroup of $\text{Aut}(D)$. Because $C = D'$, it is normal in $\text{Aut}(D)$. Now if $\alpha \in \text{Aut}(D)$

centralized C , then we could write $\iota^\alpha = \iota c^k$ for some $0 \leq k < n$. Because n is odd, we can solve $2r \equiv k \pmod{n}$, and then

$$c^{-r} \iota c^r = \iota c^{2r} = \iota c^k$$

Thus α and $c^r \in \text{Aut}(D)$ act the same way on D , and thus $\alpha = c^r$. This shows the centralizer of C is contained in C , and thus $C_{\text{Aut}(D)}(C) = C$. By Lemma 9.14, we have $|\text{Aut}(D)| \leq |C| \cdot |\text{Aut}(C)|$.

Now let $H := C \rtimes \text{Aut}(C)$ be the holomorph of C . We can consider $D \leq H$, where $\iota \in \text{Aut}(C)$ is the inversion map, so that $D = \langle C, \iota \rangle$. Now $H/C \cong \text{Aut}(C)$ is Abelian, so D/C is normal in H/C , implying $D \triangleleft H$. If $h \in H$ centralized D , then it would centralize C , and thus its image in H/C would be trivial. But then $h \in C_H(D) \cap D = Z(D) = 1$. By the N/C theorem, we have an injective homomorphism $H \rightarrow \text{Aut}(D)$. But

$$|H| = |C| \cdot |\text{Aut}(C)| \geq |\text{Aut}(D)|$$

So this map is an isomorphism, and $H \cong \text{Aut}(D)$. Note this implies $Z(H) = 1$ because $Z(D) = 1$.

Finally, let $A := \text{Aut}(H)$, and identify $H \leq A$ with the inner automorphisms. We show that $H = A$, so that the automorphism tower of D has at most two groups, namely D and H . [When $n = 3$ then $H = D \cong S_3$.] Because H/C is Abelian, and $C = D'$ is contained in H' , we have $C = H'$ is characteristic in H , hence normal in A . Choose $\alpha \in A$, and note it induces an automorphism on C . There is thus $\beta \in \text{Aut}(C) \leq H$ such that $\alpha\beta \in C_A(C)$. Then $\iota^{\alpha\beta} \in H$ acts by inversion on C , exactly as ι does, and thus

$$\iota^{\alpha\beta} \in C_H(C)\iota = C\iota \subset D$$

Thus $D^{\alpha\beta} = D$, and so we can find $h \in H = \text{Aut}(D)$ with $\alpha\beta h$ centralizing D . But Lemma 9.12 shows $C_A(D) = \{1\}$, and thus $\alpha = (\beta h)^{-1} \in H$. Since $\alpha \in A$ was arbitrary, we've successfully shown $H = A$.

There is another way to approach this problem, without giving the exact structure of $\text{Aut}(D)$. We again write $H := \text{Aut}(D)$ and $A := \text{Aut}(H)$. Our goal is to show D is normal in A , so that by [9B.2] we have $H = A$ as above. Since $C = D'$, it is characteristic in D , so normal in H . In the first paragraph we showed $C_H(C) = C$, so the N/C theorem gives an injective mapping $H/C \rightarrow \text{Aut}(C)$. But $\text{Aut}(C)$ is Abelian, so $H' \leq C = D' \leq H'$, and we have $C = H'$ is characteristic in H , hence normal in A . For $\alpha \in A$, we have that for $c \in C$

$$\iota^{-\alpha} c^\alpha \iota^\alpha = (c^\iota)^\alpha = (c^{-1})^\alpha = (c^\alpha)^{-1}$$

Thus ι^α is acting by inversion on $C^\alpha = C$, so that $[\alpha, \iota] = \iota^\alpha \iota$ centralizes C . But then

$$[\alpha, \iota] \in H \cap C_A(C) = C_H(C) = C$$

So that $\iota^\alpha \in \langle C, \iota \rangle = D$. Thus $\alpha \in N_A(D)$, and since α was arbitrary, we have $D \triangleleft A$ as desired.

[9B.5] Since $A/(A \cap G^\infty)$ is isomorphic to a subgroup of the nilpotent group G/G^∞ , it is also nilpotent, showing that $A^\infty \leq G^\infty$; similar reasoning works for B^∞ , so that we always have $A^\infty B^\infty \leq G^\infty$. If $A = G$ or $B = G$, clearly this is an equality, so we can assume throughout that A and B are proper subnormal subgroups of G , and we work to show $G^\infty \leq A^\infty B^\infty$. First we handle the case where both A and B are normal in G . Then $A^\infty B^\infty \triangleleft G$, and in the quotient we have $\overline{G} = \overline{A} \overline{B}$. Both subgroups on the right-hand side are quotients of nilpotent groups, hence nilpotent; this shows $\overline{G}$ is nilpotent as well, and thus $G^\infty \leq A^\infty B^\infty$, as desired.

Now we work via induction on $|G|$. Choose proper normal subgroups $A \leq M \triangleleft G$ and $B \leq N \triangleleft G$. Note that $G = MN$ and by the previous paragraph we have $G^\infty = M^\infty N^\infty$. But Dedekind's Lemma shows $M = A(B \cap M)$, and both of those are subnormal in M . Since $|M| < |G|$, induction shows

$$M^\infty = A^\infty (B \cap M)^\infty$$

Note that $(B \cap M)^\infty \leq B^\infty$, so that $(B \cap M)^\infty B^\infty = B^\infty$. Now $M^\infty \triangleleft G$, and thus $M^\infty B^\infty = A^\infty B^\infty$ is a subgroup containing M^∞ . Similarly, N^∞ is contained in $B^\infty A^\infty = A^\infty B^\infty$, and thus

$$G^\infty = M^\infty N^\infty \leq A^\infty B^\infty$$

9C

[9C.1] First, suppose $K < H$ in the context of Theorem 9.24. Then $D = H \cap K = K$, and no non-trivial subgroup of K is normal in H . Then $M = 1$, so $U, V \leq M$ are also trivial, which is what we're trying to show here. Thus we can assume that neither H nor K contain the other group, and in particular that both H and K are proper subgroups of G .

Suppose that $U > 1$ and $V > 1$ are both non-trivial. Then $H = N_G(U)$ and $K = N_G(V)$ by the hypotheses of Theorem 9.24. By the conclusion of that theorem, either U or V is a non-trivial p -group; without loss of generality we assume it is U . Then U is subnormal and nilpotent, so $U \leq F(G)$, implying that $1 < U \leq O_p(G)$, and thus $Z := Z(O_p(G))$ is non-trivial. But then Z centralizes U , so $Z \leq N_G(U) = H$. If V is a p -group, then $V \leq O_p(G)$ as well, so that $Z \leq N_G(V) = K$. If V is not a p -group, then $O^p(V) > 1$, and by Corollary 9.27 we have that Z normalizes $O^p(V)$ because V is subnormal. But again, the hypotheses of Theorem 9.24 imply $K = N_G(O^p(V))$, so that $Z \leq K$ in this case as well.

We've thus shown that $Z \leq H \cap K = D$ is normal in G , and that contradicts the hypotheses of Theorem 9.24. Thus it must be that $U = 1$ or $V = 1$.

[9C.2] Write $\overline{G}$ for $G/O^p(G)$, and we'll use the overbar as the homomorphism to this quotient group. Then $\overline{A}$ and $\overline{B}$ are p -groups, so we have $O^p(A)$ and $O^p(B)$ are both contained in $O^p(G)$. Thus we always have $O^p(A)O^p(B) \leq O^p(G)$, and we're trying to show the

reverse containment. Note this is trivial if $A = G$ or $B = G$, so we assume both are proper subgroups.

If A and B are both normal in G , then so is $O^p(A)O^p(B)$, and now using overbar for the homomorphism $G \rightarrow G/(O^p(A)O^p(B))$, we see that $\overline{G} = \overline{A}\overline{B}$ is a product of two (normal) p -groups, hence also a p -group. Thus $O^p(G) \leq O^p(A)O^p(B)$, as desired.

We finish via induction on $|G|$. Choose normal subgroups $A \leq M \triangleleft G$ and $B \leq N \triangleleft G$. By the previous paragraph, we have $O^p(G) = O^p(M)O^p(N)$. By Dedekind's Lemma we have $M = A(B \cap M)$, and both of those are subnormal subgroups of M . By induction then

$$O^p(M) = O^p(A)O^p(B \cap M)$$

The first paragraph showed $O^p(B \cap M) \leq O^p(B)$. Since $O^p(M)$ is normal in G , we have that $O^p(M)O^p(B) = O^p(A)O^p(B)$ is a subgroup of G containing $O^p(M)$. Similarly, we see that $O^p(N)$ is contained in $O^p(B)O^p(A) = O^p(A)O^p(B)$. We thus have

$$O^p(G) = O^p(M)O^p(N) \leq O^p(A)O^p(B)$$

[9C.3] We let G be a minimal counterexample, so that $G = \langle A, B \rangle$ and yet $G \neq AB$. Our contradiction will be in showing AB is a subgroup. We let $N \triangleleft G$ be a minimal normal subgroup, which is proper since A and B are subnormal proper subgroups.

- (a) Write $\overline{G}$ for the group G/N , and use the overbar for the homomorphism. Then $\overline{G}$ is generated by the subnormal subgroups $\overline{A}$ and $\overline{B}$. Since G is a minimal counterexample and $|\overline{G}| < |G|$, we see that $\overline{G} = \overline{A}\overline{B}$, meaning that

$$G = (AN)(BN) = (AN)(NB) = ANB$$

- (b) By Theorem 2.6, N normalizes both A and B . Thus $N \cap A$ and $N \cap B$ are normal subgroups of N , so their product is a subgroup. Obviously B normalizes $N \cap B$, and if $b \in B$ and $x \in (N \cap A)$, the fact that B and N normalize each other shows

$$[x, b] \in [N, B] \leq N \cap B$$

Thus $x^b \in x(N \cap B) \subset (N \cap A)(N \cap B)$. This shows B normalizes $(N \cap A)(N \cap B)$. Similar arguments show A does as well.

- (c) The previous part shows $G = \langle A, B \rangle$ normalizes $(N \cap A)(N \cap B) \leq N$. By minimality, either this product is trivial, or N itself. But the latter cannot be true, since then by part (a) we'd have

$$G = ANB = A(N \cap A)(N \cap B)B = AB$$

Thus $(N \cap A)(N \cap B) = \{1\}$, so each factor is trivial. But N and A normalize each other, so $[N, A] \leq N \cap A = \{1\}$, showing N centralizes A ; similarly N centralizes B . From $G = \langle A, B \rangle$ we see $N \leq Z(G)$, and minimality implies N has prime order; call that prime p .

- (d) Because $[A : A']$ and $[B : B']$ are coprime, p does not divide one of these; say p does not divide $[B : B']$. Note that if $O^p(B) < B$, then $B/O^p(B)$ would be a non-trivial p -group, which would have a non-trivial Abelianization. There would thus be a normal subgroup $O^p(B) \leq M \leq B$ such that B/M was an Abelian p -group. But then $B' \leq M$ and we'd have $[B : B']$ divisible by $[B : M]$, a power of p . This contradiction shows $O^p(B) = B$. From the previous problem we have

$$O^p(G) = O^p(A)O^p(B) = O^p(A)B$$

- (e) Because $O^p(G)$ is normal in G , $AO^p(G)$ is a subgroup of G . But from the previous part

$$AO^p(G) = AO^p(A)B = AB$$

This contradicts AB not being a subgroup, and thus our minimal counterexample G does not exist.

9D

[9D.1] Let $\mathcal{S}$ be all subnormal subgroups of G contained in X . Then $L := \langle \mathcal{S} \rangle$ is subnormal (as a join of subnormal subgroups), and is contained in X . This is clearly the unique largest one, since $S \in \mathcal{S}$ implies $S \leq L$. To see L is normal in X , note that for $x \in X$ and $S \in \mathcal{S}$, S^x is subnormal in G and is contained in $X^x = X$, and thus $S^x \in \mathcal{S}$. This shows X acts by permutations on $\mathcal{S}$ via conjugation, and thus preserves the subgroup generated by $\mathcal{S}$; that is, $L \triangleleft X$.

[9D.2] Let $\mathcal{X}$ be the set of strong conjugates of X in G . For $x \in X$, $\mathcal{X}^x$ is the set of strong conjugates of $X^x = X$. This shows X acts by permutations on $\mathcal{X}$ via conjugation, and thus X fixes their intersection. Since $X \in \mathcal{X}$, we see $L \leq X$ is a normal subgroup.

Now if $K \leq G$ is a strong conjugate of L , then we can write $K = L^g$ with g in $\langle L, L^g \rangle \leq \langle X, X^g \rangle$. This shows X^g is strongly conjugate to X , so that $L \leq X^g$. Since K is also contained in X^g , we see that L is conjugate to K within X^g . But $K = L^g$ is normal in X^g , and thus $L = K$. Since L is only strongly conjugate to itself within G , it must be subnormal (by Bartels's theorem or [2A.10]).

[9D.3] Let $G = S_4$ and let $X = \langle (1234) \rangle$ be a cyclic subgroup of order 4. Now $O_2(G) = O_2(A_4)$ is an elementary Abelian group of order 4, and thus $X \not\leq O_2(G)$. However, $(13)(24)$ is contained in both X and $O_2(G)$, so we see that $S := \{1, (13)(24)\}$ must be the subnormal core of X (here we are using that X is a 2-group, and thus every subgroup of X that is subnormal in G must be contained in $O_2(G)$). But X is the only cyclic subgroup of order 4 containing $(13)(24)$, and thus S is not the intersection of any collection of conjugates of X .

[9D.4] We call $S \leq G$ **weakly subnormal** if $S \cap P$ is a Sylow subgroup of S for every Sylow

subgroup $P \leq G$. Note that if $S \leq H \leq G$, then S is also weakly subnormal in H . To see this, let $Q \leq H$ be a Sylow subgroup, and choose a Sylow subgroup P of G containing Q . Then

$$Q \cap S = (H \cap P) \cap S = H \cap (P \cap S) = P \cap S$$

is a Sylow subgroup of S . Also, if $K \leq S$ is subnormal in S , then K is weakly subnormal in G as well. For if P is a Sylow subgroup of G , then $(P \cap S)$ is a Sylow subgroup of S , so that $P \cap S \cap K = P \cap K$ is a Sylow subgroup of K by Lemma 9.31.

Now assume that $S \leq G$ is weakly subnormal, but not subnormal. We choose the pair (G, S) such that $|G| + |S|$ is minimized. We let N be a minimal normal subgroup of G . We want to show G is simple; equivalently, that $N = G$. Now if $S \leq N$, then S is weakly subnormal in N , and $|N| < |G|$ would imply S is subnormal in N . But then S is subnormal in G , a contradiction. So $S \leq N$ implies $N = G$. We thus will assume $S \not\leq N$ and reach a contradiction.

Write $\overline{G} := G/N$ and use the overbar to denote the canonical homomorphism. All Sylow subgroups of $\overline{G}$ look like $\overline{P}$ for a Sylow subgroup $P \leq G$ by [1B.5]. Then

$$\overline{P \cap S} \leq \overline{P} \cap \overline{S}$$

By hypothesis, the left-hand side is a Sylow subgroup of $\overline{S}$, and thus we have equality and $\overline{P} \cap \overline{S}$ is a Sylow subgroup of $\overline{S}$. Thus $\overline{S}$ is weakly subnormal in $\overline{G}$, and since $|N| > 1$, we then have that $\overline{S}$ is subnormal in $\overline{G}$. This of course means that SN is subnormal in G . If $SN < G$ then S , being weakly subnormal in SN , would be subnormal in SN , implying it is subnormal in G . This contradiction shows we must have $G = SN$.

But then $S \cap N$, as a normal subgroup of S , is weakly subnormal by the first paragraph. Since we're assuming $S \not\leq N$, we know $|S \cap N| < |S|$, so $S \cap N$ is subnormal in G . It is thus normalized by the minimal subgroup N , and is hence normal in $SN = G$. Since N is minimal normal, we have $S \cap N = 1$ or $S \cap N = N$. The latter implies $G = SN = S$, which is obviously subnormal, so we must be in the case $S \cap N = 1$. Then G is really the semidirect product $N \rtimes S$. This decomposition works for any minimal normal subgroup of G . In particular, if $1 < M < S$ was minimal normal in G , we would have $G = MS = S$, a contradiction. So S contains no non-trivial normal subgroups of G .

Choose a prime p dividing $|S|$, and let Q be a Sylow p -subgroup of S . Note that $O_p(N) = 1$ or $O_p(N) = N$. In the latter case, replace p by another prime dividing $|S|$; this exists because otherwise $G = SN$ is a p -group, where every subgroup is subnormal, and that is a contradiction. If R is a Sylow p -subgroup of QN , then order considerations show R is a Sylow p -subgroup of G (since $|G| = |N| \cdot |S|$). Then $R \cap S$ is a Sylow p -subgroup of S , but

$$R \cap S \leq QN \cap S = Q(N \cap S) = Q$$

Thus Q is contained in every Sylow p -subgroup of QN , meaning that $Q \leq O_p(QN)$. Since $O_p(QN)$ is a p -group, we see that Q is subnormal in QN . From [9C.2] we then have

that

$$O_p(QN) = O_p(Q)O_p(N) = Q$$

So $N \leq QN$ normalizes Q . But then $[Q, N] \leq Q \cap N \leq S \cap N = \{1\}$. Thus $Q \leq C_S(N)$. But $C_S(N)$ is normal in S , and is of course normalized by N , so $C_S(N) \triangleleft G$. From the previous paragraph, we have $C_S(N) = \{1\}$, and this is our final contradiction.

So we've shown G is simple. Since all subgroups are (sub)normal in an Abelian group, G must be non-Abelian. If $1 < M \triangleleft S$, then from the first paragraph M is weakly subnormal in G , so that if $M < S$ we would have M subnormal in G . But G is simple, so this is impossible. Then $M = S$ and we see S is simple as well. If S was Abelian, it would be of order p for some prime p . Then by hypothesis S would be contained in every Sylow p -subgroup of G , implying $O_p(G) > 1$. Thus we must have that S is non-Abelian as well.

10A

[10A.1] Assume the result is false, and let P be a non-Abelian regular 2-group such that $|P|$ is minimized. We reach a contradiction to show the result is true.

First note that quotients of regular groups are regular. To see this, let $\bar{P}$ be a quotient of P , and let $\bar{x}, \bar{y} \in \bar{P}$, with $x, y \in P$. If we write $H := \langle x, y \rangle$, then by the regularity of P there is an element $c \in [H, H]$ with $(xy)^p = x^p y^p c^p$. But $\bar{H} = \langle \bar{x}, \bar{y} \rangle$, and $\bar{c} \in [\bar{H}, \bar{H}] = [\bar{H}, \bar{H}]$. Since $(\bar{x}\bar{y})^p = \bar{x}^p \bar{y}^p \bar{c}^p$ in $\bar{P}$, we see $\bar{P}$ is regular.

Back to our minimal counterexample P . If N is any non-trivial normal subgroup of P , then P/N is regular, and from $|P/N| < |P|$ we see that P/N is Abelian. In particular, $P' \leq N$. If we take $N \leq Z(P)$ of order 2, this shows $|P'| \leq 2$. Since P is non-Abelian, we have P' of order 2. But then, for $x, y \in P$, regularity implies

$$(xy)^2 = x^2 y^2 c^2 = x^2 y^2$$

where the last equality follows because $c \in P'$ has order dividing $|P'| = 2$. But this equation shows

$$yx = x^{-1}(xy)^2 y^{-1} = x^{-1}(x^2 y^2) y^{-1} = xy$$

Thus P is actually Abelian, and that's our contradiction.

[10A.2] Assume the result is false, and let P be a regular p -group where $K(P) = \{x \in P \mid x^p = 1\}$ is not a subgroup. Choose P such that $|P|$ is minimized over all counterexamples. We will reach a contradiction, establishing the result is true.

First, note that subgroups of regular groups are regular. This follows because if $x, y \in H \leq P$, then $\langle x, y \rangle \leq H$ as well, showing that there exists $c \in \langle x, y \rangle'$ with $(xy)^p = x^p y^p c^p$. The minimality of $|P|$ then means that $K(H)$ is a subgroup of H for all proper subgroups $H < P$.

Let $x \in K(P)$. Then for any $y \in P$, we have that x and x^y are contained in a proper subgroup of P ; to see this, note that if $x \in M$ for a maximal subgroup $M \triangleleft P$, then $x^y \in M$ as well. So the only way this can fail is if x is contained in no maximal subgroup, implying $P = \langle x \rangle$ is cyclic, in which case $K(P)$ is clearly a subgroup. Thus we have $x, x^y \in H < P$, and since $x, x^y \in K(H)$, we have that $[x, y] = x^{-1}x^y \in K(H)$ as well. Thus all such commutators have order p , and thus all belong to $K(P')$, which is a subgroup since $P' < P$.

Now let $x, y \in K(P)$. If $L := \langle x, y \rangle < P$, then $x, y \in K(L)$, and since it's a subgroup, we have $xy \in K(L)$, so that $(xy)^p = 1$ and thus $xy \in K(P)$. Since we're assuming $K(P)$ is not a subgroup, we must have $x, y \in K(P)$ with $P = \langle x, y \rangle$, and $(xy)^p \neq 1$. By the previous paragraph establishing $K(P')$ as a subgroup, and the commutator identity $[ab, c] = [a, c]^b [b, c]$, we see that all commutators in P are of order p , so that $P' = K(P')$. But then by regularity we have $c \in P'$ with

$$1 \neq (xy)^p = x^p y^p c^p = c^p = 1$$

where the last equality follows from $c \in P' = K(P')$. This is our contradiction.

[10A.3] By hypothesis, we can write $A = Z(P) \times Q$ for a subgroup $Q \leq A$. [10A.5] shows that P is isomorphic to a subgroup of $H := C_p \wr C_p$. Now note that $P' \leq H'$, which is elementary Abelian. Lemma 4.6 says

$$P' \cong A / (A \cap Z(P)) = A / Z(P) \cong Q$$

Thus Q is elementary Abelian, and so is A .

[10A.4] Let $Q_8 = \langle i, j \rangle$ and $C_2 = \langle c \rangle$. Then $\Phi(P) = P' = \langle i^2 \rangle$ and $Z := Z(P) = \langle i^2, c \rangle$. In particular, note that $[Z : P'] = 2$. Since $|P| = 16$ and $D_8 \cong C_2 \wr C_2$ has order 8, we can show P doesn't have D_8 as a quotient by looking at P/M for all normal subgroups M of order 2. This means $M \leq Z(P)$, and we see

- P/P' is Abelian, so not isomorphic to D_8 ;
- $P/C_2 \cong Q_8$ is not isomorphic to D_8 ;
- $P/\langle i^2 c \rangle$ has a unique element of order 2, so is not isomorphic to D_8 .

Thus P does not have D_8 as a quotient, so by Yoshida's Transfer theorem, $N := N_G(P) \leq G$ controls 2-transfer. Thus, to show $G' < G$, it is enough to show that $A^2(N) < N$. The benefit of shifting to N is that $P \triangleleft N$.

By the Schur-Zassenhaus theorem, we can find a complement $H \leq N$ to P , so that $N = PH$ and $|H|$ is coprime to p . If $ph \in PH$ and $q \in P$, then commutator identities and the fact $P' \triangleleft N$ show

$$[ph, q] = [p, q]^h [h, q] \in P'[H, P]$$

If $F \leq P$ is the focal subgroup of P in N , then the above shows $F = P'[H, P]$. By the Focal Subgroup theorem, if we can show $F < P$, then $A^p(N) < N$.

Now we look at H acting on $\bar{P} := P/P'$, an elementary Abelian group of order 8. Since $\bar{Z}$ has order 2 and is characteristic, H fixes $\bar{Z}$, and thus fixes it pointwise. This shows $1 < \bar{Z} \leq C_{\bar{P}}(H)$. But we can write $\bar{P} = C_{\bar{P}}(H) \times [H, \bar{P}]$ by Theorem 4.34, and thus we must have $[H, \bar{P}]$ is a proper subgroup. Then

$$\bar{F} = \overline{[H, P]} = [H, \bar{P}] < \bar{P}$$

so that F is a proper subgroup of P , as desired.

[10A.5] Suppose $N \leq Q$ is a non-trivial normal subgroup of P . Then since P is a p -group we have

$$1 < N \cap Z(P) = N \cap Q \cap Z(P) \leq Q \cap Z(P) = 1$$

This contradiction shows N must be trivial, so that Q is core-free in P . The action of P on the cosets of Q then gives an embedding of P into S_{p^2} . Then P is contained in a Sylow p -subgroup of S_{p^2} , which is $C_p \wr C_p$.

[10A.6] Let H be the point stabilizer of $\alpha \in \Omega$. First suppose G is 2-transitive, and pick a $g \in G \setminus H$ with $\alpha \cdot g = \beta$. Now pick any element $x \in G$. If x fixes α , then $x \in H$. Otherwise, let $\alpha \cdot x = \gamma$ (where we allow $\beta = \gamma$). Since H is transitive on $\Omega \setminus \{\alpha\}$, pick an $h \in H$ with $\gamma \cdot h = \beta$. Then

$$\alpha \cdot (xhg^{-1}) = \gamma \cdot (hg^{-1}) = \beta \cdot g^{-1} = \alpha$$

Thus $xhg^{-1} \in H$, so $x \in HgH$. Because $x \in G$ was arbitrary, we have established that $G = H \cup HgH$.

Conversely, suppose $G = H \cup HgH$. If $g \in H$, then $G = H$ which is nonsensical as G is transitive, and 2-transitivity only makes sense when $|\Omega| > 1$. So let $\alpha \cdot g = \beta$. Let $\gamma \neq \alpha$ be arbitrary, and pick an $x \in G$ with $\alpha \cdot x = \gamma$. Then $x \in HgH$ and we can write $x = h_1gh_2$. But then

$$\gamma = \alpha \cdot x = \alpha \cdot (h_1gh_2) = \alpha \cdot (gh_2) = \beta \cdot h_2$$

This shows that β and γ are in the same H -orbit. Since γ was an arbitrary element in $\Omega \setminus \{\alpha\}$, we see that H acts transitively on that set, so G is 2-transitive.

[10A.7] Let $x \in P \setminus A$ be of order p , and $y \in P \setminus A$ have order p^2 . Then we can write $y = x^i a$ for $0 \leq i < p$ and $a \in A$. Since x^i also has order p , we can replace x with x^i so that $y = xa$. Finally, we let $T = \{x^{-1}, \dots, x^{-p}\}$ be a transversal for A in P .

Let $V : P \rightarrow A$ be a pre-transfer map. By Lemma 10.6 we can write

$$V(a) = \prod_{t \in T} x^t = (xax^{-1})(x^2ax^{-2}) \dots (x^pax^{-p}) = (xa)^p x^{-p} = (xa)^p$$

Since xa has order p^2 , we see $V(a) \neq 1$. Since $\Phi(A) = \{1\}$, Lemma 10.7 then shows that $C_p \wr C_p$ is a homomorphic image of P .

10B

[10B.1] Let $\sigma \in \text{Aut}(C)$ be such that $x^\sigma = x^{1+p}$. Now, by the binomial theorem, we can write

$$(1 + kp^m)^p = 1 + \sum_{i=1}^{p-1} \binom{p}{i} k^i p^{im} + k^p p^{pm}$$

All the binomial coefficients are divisible by p , and of course $p > 1$, so that we've shown $(1 + kp^m)^p \equiv 1 \pmod{p^{m+1}}$. This fact, together with induction, shows

$$(1 + p)^{p^m} \equiv 1 \pmod{p^{m+1}}$$

This implies that $|\sigma|$ divides p^{n-1} , and thus is a power of p . Thus the group $P = C \rtimes \langle \sigma \rangle$ is indeed a p -group.

Of course, $C \triangleleft P$ and $P/C \cong \langle \sigma \rangle$, so P is metacyclic. If $y \in C$ is such that $y^\sigma = y$, then $y^p = 1$. Since there is a unique subgroup of order p in C , we see that $C \cap C_P(\sigma)$ has order p . But

$$1 < C \cap Z(P) \leq C \cap C_P(\sigma)$$

so that $C \cap Z(P)$ has order p . Theorem 4.7 then shows P has nilpotence class n .

[10B.2] Write S for the socle of G , and let $|E| = p^n$; we proceed by induction on n . If $n = 1$, then E is a minimal normal subgroup of G , so E is contained in S . Now assume it's true for all $m < n$. If E is minimal normal, then again $E \leq S$. Otherwise, G acts on E via conjugation, and this action is equivalent to the one by $H := G/C_G(E)$. If $N \leq E$ is a minimal normal subgroup of G , then Maschke's theorem implies there's a subgroup $K \leq E$ which is H -invariant and $E = N \times K$. Then $K \triangleleft G$ is elementary Abelian, and $|K| < |E|$. The inductive hypothesis implies $K \leq S$, and of course $N \leq S$, so $E = NK \leq S$.

10C

[10C.1] We first define the map $\theta : \mathbb{Z}[G] \rightarrow \mathbb{Z}[H]$ by

$$\theta \left(\sum_{g \in G} c_g g \right) = \sum_{g \in G} c_g \phi(g)$$

This is well-defined because G is a $\mathbb{Z}$ -basis for $\mathbb{Z}[G]$, and it is clearly a homomorphism of additive groups. If $x, y \in G$ we have for $m, n \in \mathbb{Z}$

$$\theta(mxn y) = \theta(mnxy) = mn\phi(xy) = mn\phi(x)\phi(y) = m\phi(x)n\phi(y) = \theta(mx)\theta(ny)$$

Thus θ preserves the multiplication, and since $\theta(1) = \phi(1) = 1$, we see that θ is indeed a ring homomorphism.

We let $N := \ker(\phi)$ and $J := \ker(\theta)$. Now if $z := \sum a_n n$ is contained in $\Delta(N)$, then we have

$$\theta(z) = \theta\left(\sum_{n \in N} a_n n\right) = \sum_{n \in N} a_n \phi(n) = \sum_{n \in N} a_n = \delta(z) = 0$$

Here we've used that $\phi(n) = 1$ for all $n \in N$. This shows $\Delta(N) \subset J$, and since $J \leq \mathbb{Z}[G]$ is an ideal, we have that $\Delta(N)\mathbb{Z}[G]$ and $\mathbb{Z}[G]\Delta(N)$ are both contained in J . These are in fact equal, of course, as shown by

$$\begin{aligned} \left(\sum_{n \in N} a_n n\right) \left(\sum_{g \in G} c_g g\right) &= \sum_{g \in G} \left(\sum_{n \in N} a_n c_{n^{-1}g}\right) g \\ &= \sum_{g \in G} \left(\sum_{n \in N} a_n c_{gn^{-g}}\right) g && (n^{-1}g = gn^{-g}) \\ &= \left(\sum_{g \in G} c_g g\right) \left(\sum_{n \in N} a_n n^g\right) && (N \triangleleft G) \end{aligned}$$

So to finish, we show that $J \leq \Delta(N)\mathbb{Z}[G]$. Suppose $r := \sum c_g g$ is in J , so that $\theta(r) = 0$. Now for any $h \in \text{Im}(\phi)$, pick a $g_h \in \phi^{-1}(h)$, which is just a right coset of N . Because H is a $\mathbb{Z}$ -basis for $\mathbb{Z}[H]$, the coefficient of h in $\theta(r)$ is zero. But this coefficient is

$$\sum_{g \in \phi^{-1}(h)} c_g = \sum_{n \in N} c_{ng_h}$$

Thus $r_h := (\sum c_{ng_h} n)g_h \in \Delta(N)\mathbb{Z}[G]$. But G is a disjoint union of these cosets as h iterates over $\text{Im}(\phi)$, and we have

$$r = \sum_{g \in G} c_g g = \sum_{h \in \text{Im}(\phi)} \sum_{n \in N} c_{ng_h} n g_h = \sum_{h \in \text{Im}(\phi)} \left(\sum_{n \in N} c_{ng_h} n\right) g_h = \sum_{h \in \text{Im}(\phi)} r_h$$

so that $r \in \Delta(N)\mathbb{Z}[G]$, as desired.

[10C.2] Let p be a prime number, and note that A/pA is a finitely generated Abelian group where every element has order dividing p . Thus A/pA is a finite elementary Abelian group, say of order p^n . Now if $\{a_1, \dots, a_m\} \subset A$ is a $\mathbb{Z}$ -basis for A , then $\{\bar{a}_1, \dots, \bar{a}_m\}$ is also a generating set for A/pA , so $n \leq m$. If there existed integers $\{c_i\}$ with $0 \leq c_i < p$, and we could write

$$\sum c_i \bar{a}_i = 0$$

Then up in A that would imply the existence of integers k_i such that

$$\sum c_i a_i = \sum p k_i a_i$$

Since the $\{a_i\}$ form a $\mathbb{Z}$ -basis for A , this implies that $c_i = p k_i$, and being divisible by p (plus the bounds for c_i established above) implies $c_i = 0$. This holds for all $1 \leq i \leq m$, and

thus $\{\bar{a}_1, \dots, \bar{a}_m\}$ is linearly independent in A/pA , so $n \geq m$. Thus we have $n = m$, and we see that the size of any $\mathbb{Z}$ -basis of A is determined by the basis-independent invariant $|A/pA|$.

[10C.3] Let $h \in H$. Since $\delta(1) = 1$, and h is invertible, we see that $\delta(h) \in \mathbb{Z}$ is invertible, so that $\delta(h) = \pm 1$. Define a map ψ from U to U by sending $u \mapsto \delta(u)u$, and also define $K := \psi(H)$. Since this is only potentially changing the sign of elements of H , we see that K is still a $\mathbb{Z}$ -basis of $\mathbb{Z}[G]$. Also, for $k \in K$, we can write $k = \delta(h)h$ for some $h \in H$, and then

$$\delta(k) = \delta(\delta(h)h) = \delta(h)^2 = 1$$

All that's left then is to show $H \cong K$. Now if $\psi(h_1) = \psi(h_2)$, then $\delta(h_1)\delta(h_2)^{-1}h_1 = h_2$; since H is a $\mathbb{Z}$ -basis for $\mathbb{Z}[G]$ this already implies $h_1 = h_2$. Thus ψ is injective on H . Once we show ψ is a group homomorphism, we will then be done. For that we have

$$\psi(uv) = \delta(uv)uv = \delta(u)\delta(v)uv = \delta(u)u\delta(v)v = \psi(u)\psi(v)$$

[10C.4] By the previous exercise, we can assume that H is such that $\delta(h) = 1$ for all $h \in H$. Let $I := \Delta(G)$ be the kernel of the augmentation homomorphism. Then $h - 1 \in I$ for all $h \in H$, and we define a map $\theta : H \rightarrow I$ by setting $\theta(h) = h - 1$. We compose it with the canonical map $I \rightarrow I/I^2$ to get a map $\phi(h) = \overline{h - 1}$. To see this is a homomorphism (where I/I^2 is an Abelian group under addition), we have

$$\theta(hk) = (hk - 1) = (h - 1) + (k - 1) + (h - 1)(k - 1) \equiv (h - 1) + (k - 1) = \theta(h) + \theta(k) \pmod{I^2}$$

Thus $\phi(hk) = \phi(h) + \phi(k)$. Since H is a $\mathbb{Z}$ -basis, for $x \in I$ we can write $x = \sum c_h h$. But then

$$0 = \delta(x) = \sum_{h \in H} c_h \delta(h) = \sum_{h \in H} c_h$$

Thus we can also write $x = \sum c_h (h - 1)$, showing $x \in \theta(H)$. So ϕ is surjective, and by Theorem 10.20 we know that $I/I^2 \cong G/G'$. So we will be done if we can show $\ker(\phi) = H'$. Clearly $H' \leq \ker(\phi)$; we show the reverse containment. We write $H^\# := H \setminus \{1\}$. Now the set $\{(h - 1) \mid h \in H^\#\}$ spans I from what was shown above, and is also $\mathbb{Z}$ -linearly independent because H is a $\mathbb{Z}$ -basis. Thus $\{(h - 1) \mid h \in H^\#\}$ is a $\mathbb{Z}$ -basis for I , and we can define an Abelian group homomorphism $\psi : I \rightarrow H/H'$ by sending $(h - 1) \mapsto H'h$. We have that

$$\psi((h - 1)(k - 1)) = \psi((hk - 1) - (h - 1) - (k - 1)) = H'(hk)H'h^{-1}H'k^{-1} = H'[h^{-1}, k^{-1}] = H'$$

Since elements of the form $(h - 1)(k - 1)$ generate I^2 as an Abelian group, we see that $I^2 \subset \ker(\psi)$. Now let $h \in \ker(\phi)$. Then $\theta(h) \in I^2$, and thus $H'h = \psi(\theta(h)) \in \psi(I^2) = H'$. This shows $h \in H'$ so that $\ker(\phi) \leq H'$ and we're done.

[10C.5] Let e be the coefficient of 1 in α . Then e is the coefficient of g_i in $g_i \alpha$ for all $g_i \in G$: to see this, note that $g_i g = g_i$ implies $g = 1$. Thus the diagonal elements of $M(\alpha)$ are all e , so the trace is simply $e|G| = ne$.

[10C.6]

Define the mapping $\Xi : \mathbb{Z}[G] \rightarrow \text{Mat}_n(\mathbb{Z})$ by using the definition in the previous problem: $\Xi(x) = M(x)$. Let $M := \Xi(\alpha)$, $N := \Xi(\beta)$, and $P := \Xi(\alpha\beta)$ for $\alpha, \beta \in \mathbb{Z}[G]$. We also let $M = \{m_{ij}\}$ and similarly for N and P . We then compute that

$$g_i(\alpha\beta) = \left(\sum_{j=1}^n m_{ij} g_j \right) \beta = \sum_{j=1}^n m_{ij} \sum_{k=1}^n n_{jk} g_k$$

Thus $P_{ik} = \sum_j m_{ij} n_{jk}$. But this is just $(MN)_{ik}$, and so $P = MN$. That is, Ξ preserves multiplication (in fact, it is a ring homomorphism). Now assuming that $\alpha^m = 1$, we can use this map to show $I = \Xi(\alpha^m) = M^m$; note this means M is an invertible matrix. Viewing M as a matrix over $\mathbb{C}$, let ϵ be an eigenvalue of M with associated eigenvector $w \in \mathbb{C}^n$. Then

$$w = wM^m = w\epsilon^m$$

Thus $\epsilon^m = 1$, and all eigenvalues of M are m th roots of unity. But if $\{\epsilon_1, \dots, \epsilon_n\}$ are the eigenvalues of M (counted with multiplicity), we have by the previous problem

$$|ne| = \left| \sum_{i=1}^n \epsilon_i \right| \leq \sum_{i=1}^n |\epsilon_i| = n$$

Thus $|e| \leq 1$, as desired.