SOLUTIONS FOR FINITE GROUP THEORY BY I. MARTIN ISAACS

Abstract. Use at your own risk.

1A

1. We have a homomorphism $\sigma : G \to S_p$ with $\ker\sigma = \mathrm{core}_G(H)$. So $\left|G/\mathrm{core}_G(H)\right|$ divides $p!$ (by first isomorphism theorem).

Suppose $\mathrm{core}_G(H) \subsetneq H$. Then there is a prime number q which divides $|H : \mathrm{core}_G(H)|$. In particular q divides $|G|$, so $q \geq p$. Since

$$\left|G/\mathrm{core}_G(H)\right| = |G : H||H : \mathrm{core}_G(H)| = p\,|H : \mathrm{core}_G(H)|,$$

we conclude that pq divides $p!$, so q divides $(p-1)!$. This is impossible because $q > p-1$ and q is prime. Thus $\mathrm{core}_G(H) = H$. $H \trianglelefteq G$.

2. Note that $HgK = \bigcup_{k\in K} Hgk$. Consider the set $X = \{Hgk : k \in K\}$. K acts on X by right multiplication, clearly this action is transitive. We compute the stabilizer of $Hg \in X$ under this action:

$$\begin{aligned}\mathrm{stab}_K(Hg) &= \{k \in K : Hgk = Hg\}\\ &= \{k \in K : gkg^{-1} \in H\}\\ &= \{k \in K : k \in H^g\}\\ &= K \cap H^g\end{aligned}$$

The orbit-stabilizer theorem gives $|X| = |K : K \cap H^g|$. Lastly, observe that HgK is precisely the union of the elements of X. Since distinct elements of X are disjoint and all have size $|H|$, we have

$$|HgK| = |H||X| = \frac{|H||K|}{|K \cap H^g|}$$

3. a) The subset $HK \subseteq G$ has size

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

So

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

with equality if and only if $|HK| = |G|$, i.e. $HK = G$.

b) $|G : K|$ divides $|G : H \cap K| = |G : H||H : H \cap K|$. Since $|G : K|$ and $|G : H|$ are coprime, $|G : K|$ divides $|H : H \cap K|$. In particular $|G : K| \leq |H : H \cap K|$. We always have the reverse inequality by (a). So we get equality and again by (a) we conclude $HK = G$.

4. Let $g \in G$. Write $g = hk$ with $h \in H$, $k \in K$. Then

$$H^gK = H^{hk}K = H^kK = k^{-1}HkK = k^{-1}HK = k^{-1}KH = KH = G$$

Now let $x, y \in G$. By above $H^{xy^{-1}}K = G$.
Hence $G = G^y = (H^{xy^{-1}}K)^y = H^xK^y$.

5. Assume $G_\alpha G_\beta = G$ for some $\alpha \in \Omega$, $\beta \in \Lambda$. Pick an arbitrary element (α', β') from $\Omega \times \Lambda$. We will show that (α', β') and (α, β) lie in the same orbit, which is sufficient for showing that the action

on $\Omega \times \Lambda$ is transitive.
We know that there exists $g \in G$ such that $\alpha' \cdot g = \alpha$. So $(\alpha', \beta') \cdot g = (\alpha, \beta' \cdot g)$.
Now pick $g' \in G$ such that $(\beta' \cdot g) \cdot g' = \beta$. Then $(\alpha, \beta' \cdot g) \cdot g' = (\alpha \cdot g', \beta)$. Write $g' = ab$ with $a \in G_\alpha$, $b \in G_\beta$.
We have

$$(\alpha \cdot g', \beta) = (\alpha \cdot b, \beta) = (\alpha \cdot b, \beta) = (\alpha \cdot b, \beta \cdot b) = (\alpha, \beta) \cdot b$$

Shortly, $(\alpha', \beta') \cdot gg' = (\alpha \cdot g', \beta) = (\alpha, \beta) \cdot b$. We are done.
For the converse, assume the action of G on $\Omega \times \Lambda$ is transitive. Fix $\alpha \in \Omega$, $\beta \in \Lambda$. Let $g \in G$. Consider the elements (α, β) and $(\alpha \cdot g, \beta)$ in $\Omega \times \Lambda$. By transitivity there exists $b \in G$ such that $(\alpha, \beta) \cdot b = (\alpha \cdot g, \beta)$.
So $\alpha \cdot b = \alpha \cdot g$ and $\beta \cdot b = \beta$, that is $gb^{-1} \in G_\alpha$ and $b \in G_\beta$. Thus $g = gb^{-1}b \in G_\alpha G_\beta$. $g \in G$ was arbitrary, it follows that $G = G_\alpha G_\beta$.

6. Consider the set $X = \{(g, \alpha) : \alpha \cdot g = \alpha\} \subseteq G \times \Omega$. We compute $|X|$ in different ways. Firstly,

$$|X| = \sum_{g \in G} |\{\alpha \in \Omega : \alpha \cdot g = \alpha\}| = \sum_{g \in G} \chi(g)$$

Secondly, using orbit-stabilizer theorem:

$$|X| = \sum_{\alpha \in \Omega} |\{g \in G : \alpha \cdot g = \alpha\}| = \sum_{\alpha \in \Omega} |G_\alpha| = \sum_{\alpha \in \Omega} \frac{|G|}{|\mathcal{O}_\alpha|} = |G| \sum_{\alpha \in \Omega} \frac{1}{|\mathcal{O}_\alpha|},$$

where $\mathcal{O}_\alpha$ denotes the orbit of α.
Say Ω is partitioned into orbits as $\Omega = \mathcal{O}_1 \sqcup \cdots \sqcup \mathcal{O}_n$. Then,

$$\sum_{\alpha \in \Omega} \frac{1}{|\mathcal{O}_\alpha|} = \sum_{i=1}^{n} \sum_{\alpha \in \mathcal{O}_i} \frac{1}{|\mathcal{O}_\alpha|} = \sum_{i=1}^{n} \sum_{\alpha \in \mathcal{O}_i} \frac{1}{|\mathcal{O}_i|} = \sum_{i=1}^{n} \left(\frac{1}{|\mathcal{O}_i|} \sum_{\alpha \in \mathcal{O}_i} 1 \right) = \sum_{i=1}^{n} \left(\frac{1}{|\mathcal{O}_i|} |\mathcal{O}_i| \right) = n$$

Thus $|X| = n|G|$.

7. The action of G on the right cosets of H (by right multiplication) is clearly transitive, hence

$$\sum_{g \in G} \chi(g) = |G|$$

by 1A.6.
Let $g \in G - H$. Under the induced action of H on the right cosets of H, H and Hg are in different orbits. So there are at least 2 orbits and we conclude that

$$\sum_{h \in H} \chi(h) \geq 2|H|$$

again by 1A.6.
Let $S = \{g \in G : \chi(g) = 0\}$. Since

$$\chi(g) = \{Ha : Hag = Ha\} = \{Ha : aga^{-1} \in H\} = \{Ha : g \in H^a\},$$

S is exactly the set of elements in G that are not contained in any conjugate of H.
We also see that for every $h \in H$, $\chi(h)$ contains H, so $\chi(h) \neq 0$. In other words, $H \subseteq G - S$. Now,

$$\begin{aligned} |G| = \sum_{g \in G} \chi(g) = \sum_{g \in G - S} \chi(g) = \sum_{g \in H} \chi(g) + \sum_{g \in (G-S)-H} \chi(g) \\ \geq 2|H| + |G - (S - H)| \end{aligned}$$

Since $|G - (S - H)| = |G - (S \cup H)| = |G| - |S \cup H|$, we obtain $|S \cup H| \geq 2|H|$.
Noting that $|S| + |H| \geq |S \cup H|$, we get $|S| \geq |H|$, which is the desired result.

8. a) I give a 'high-brow' argument for fun. Firstly, observe that if $x_1 x_2 \ldots x_n = 1$, we have $x_1^{-1} = x_2 \ldots x_n$, hence $x_2 \ldots x_n x_1 = 1$. So we have a function

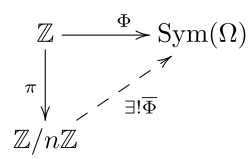
$$\sigma : \Omega \to \Omega$$

$$(x_1, x_2, \ldots, x_n) \mapsto (x_2, \ldots, x_n, x_1)$$

It is easily checked that σ is a bijection (Basically, σ is a 'left-shift' and the 'right-shift' is its inverse). Therefore $\sigma \in \mathrm{Sym}(\Omega)$.
$\mathbb{Z}$ is the free group with a single generator, so there is a unique group homomorphism $\Phi : \mathbb{Z} \to \mathrm{Sym}(\Omega)$ such that $\Phi(1) = \sigma$.
Noting the group operation is written additively in $\mathbb{Z}$, we have

$$\Phi(n) = \Phi(n \cdot 1) = (\Phi(1))^n = \sigma^n = 1_{\mathrm{Sym}(\Omega)}$$

So $n \in \ker\Phi$, hence $n\mathbb{Z} \subseteq \ker\Phi$.
By the universal property of quotients, there is a unique group homomorphism $\overline{\Phi} : \mathbb{Z}/n\mathbb{Z} \to \mathrm{Sym}(\Omega)$ making the diagram



commute, where π is of course the canonical projection. This means $\mathbb{Z}/n\mathbb{Z}$ acts on Ω via (we denote $\pi(k)$ by $\overline{k}$)

$$\begin{aligned}(x_1, \ldots, x_n) \cdot \overline{k} &= \overline{\Phi}(\overline{k})(x_1, \ldots, x_n) \\ &= \Phi(k)(x_1, \ldots, x_n) \\ &= (\Phi(1))^k(x_1, \ldots, x_n) \\ &= (x_{1+k}, \ldots, x_{n+k})\end{aligned}$$

where subscripts are interpreted modulo n.

b) Let $\Omega_0 \subseteq \Omega$ be the set of fixed points of the action. Clearly if $x \in G$ with $x^p = 1$, $(x, x, \ldots, x) \in \Omega_0$. Conversely if $(x_1, \ldots, x_p) \in \Omega_0$,

$$(x_1, \ldots, x_p) = \sigma(x_1, \ldots, x_p) = (x_2, \ldots, x_p, x_1)$$

and we get $x_1 = x_2 = \cdots = x_p$.
Hence $\Omega_0 = \{(x, x, \ldots, x) : x \in G, x^p = 1\}$.
p is prime, so the group which is acting on Ω as in (a) (namely $\mathbb{Z}/p\mathbb{Z}$) is a p-group.
It is worth noting that in general when a p-group acts on a set Ω, with Ω_0 being the set of fixed points of the action, we have

$$|\Omega| \equiv |\Omega_0| \pmod p$$

(Much of Sylow theory stems from this actually)
In our case $|\Omega| = |G|^{p-1}$ because we can choose $x_1, \ldots, x_{p-1}$ in any way we want and then they uniquely determine $x_p = (x_1 \ldots x_{p-1})^{-1}$.
Since p divides $|G|$, we get

$$0 \equiv |\Omega| \equiv |\Omega_0| \pmod p$$

Observe that since p is prime, $\Omega_0 = \{(1, 1, \ldots, 1)\} \cup \{(x, x, \ldots, x) : |x| = p\}$. Thus

$$|\{x : |x| = p\}| = |\{(x, x, \ldots, x) : |x| = p\}| \equiv -1 \pmod p$$

9. Suppose G has two different subgroups, say H and K, of order p. p is prime, so $H \cap K = 1$. Thus

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

which gives $m \geq p$, a contradiction. So there is *at most* one subgroup of order p. Cauchy's theorem guarantees that there is *at least* one such subgroup. The statement follows.

10. a) Let Ω be the set of right cosets of H. H acts on Ω by right multiplication. Denoting the set of fixed points by Ω_0, we have:

$$\begin{aligned}\Omega_0 &= \{Ha : Hah = Ha \text{ for all } h \in H\} \\ &= \left\{Ha : aha^{-1} \in H \text{ for all } h \in H\right\} \\ &= \left\{Ha : aHa^{-1} \subseteq H\right\} \\ &= \{Ha : H^a = H\} \\ &= \{Ha : a \in N_G(H)\}\end{aligned}$$

Therefore $|\Omega_0| = |\mathbf{N}_G(H) : H|$, as desired.

b) Note that $|\Omega| = |G : H|$. If H is a p-subgroup, we have

$$\begin{aligned}|\Omega| &\equiv |\Omega_0| \pmod p \\ |G : H| &\equiv |\mathbf{N}_G(H) : H| \pmod p\end{aligned}$$

The assertion follows.

1B

1. a) $|PS| = \frac{|P||S|}{|P \cap S|}$ is a power of p. So if PS is a subgroup, it is a p-subgroup which contains $S \in \mathrm{Syl}_p(G)$. Hence $PS = S$, so $P \subseteq S$.
The converse implication is trivial.

b) Let $T \in \mathrm{Syl}_p(G)$. Since $S \trianglelefteq G$, TS is a subgroup of G. As T is a p-subgroup, by (a) we have $T \subseteq S$. But $|T| = |S|$, so $T = S$.
This shows that $\mathrm{Syl}_p(G) = \{S\}$. So writing $|G| = p^a m$ with $p \nmid m$, S is the unique subgroup of G of order p^a. Hence S is characteristic in G.

2. We know $\mathbf{O}_p(G)$ is a normal p-subgroup of G.
Let P be a normal p-subgroup of G. Then for all $S \in \mathrm{Syl}_p(G)$, PS is a subgroup of G. By 1B.1.a, we get $P \subseteq S$ for all $S \in \mathrm{Syl}_p(G)$. Hence

$$P \subseteq \bigcap_{S \in \mathrm{Syl}_p(G)} S = \mathbf{O}_p(G)$$

3. $S \trianglelefteq \mathbf{N}_G(S) = N$. S is also a Sylow p-subgroup of N. By (1.a) S is characteristic in N. As N is normal in $\mathbf{N}_G(N)$, S is normal in $\mathbf{N}_G(N)$.
Therefore by the definition of the normalizer, we have $\mathbf{N}_G(N) \subseteq \mathbf{N}_G(S) = N$.
Thus $N = \mathbf{N}_G(N)$.

4. By 1A.10, $|\mathbf{N}_G(P) : P|$ is divisible by p. $P \trianglelefteq \mathbf{N}_G(P)$, so the order of the factor group $\mathbf{N}_G(P)/P$ is divisible by p.
By Cauchy's theorem, $\mathbf{N}_G(P)/P$ has a subgroup Q/P of order p. Here Q is a subgroup of $\mathbf{N}_G(P)$ containing P such that $|Q : P| = p$.
Now let M be a maximal p-subgroup of G (with respect to inclusion). Suppose $|G : M|$ is divisible by p. But then by above we get a subgroup Q of G such that $M \subseteq Q$ and $|Q : M| = p$. That is, Q is a p-subgroup of G strictly containing M, contradicting the maximality of M.
Thus $|G : M|$ is not divisible by p. It follows that M is a Sylow p-subgroup of G.

5. a) Consider the restriction $\theta|_H : H \to \theta(H)$. $\theta|_H$ is a surjective group homomorphism with kernel $\ker\theta \cap H$, thus

$$\theta(H) \cong \frac{H}{\ker\theta \cap H}$$

In particular $|\theta(H)|$ divides $|H|$, so every prime dividing $|\theta(H)|$ also divides $|H|$, hence is in π.
We have $K \cong {}^{G}/_{\ker\theta}$ as θ is surjective. Then

$$|K : \theta(H)| = \frac{|G|}{|\ker\theta|} \cdot \frac{|\ker\theta \cap H|}{|H|} = \frac{|G : H|}{|\ker\theta : \ker\theta \cap H|}$$

So $|K : \theta(H)|$ divides $|G : H|$. Now if p is a prime dividing $|K : \theta(H)|$, then p divides $|G : H|$, hence $p \notin \pi$.
Done.

b) Let $P \in \mathrm{Syl}_p(K)$. Consider the subgroup $A = \theta^{-1}(P)$ of G. Note that $\ker\theta \subseteq A$ and since θ is surjective $\theta(A) = P$. Thus $P = \theta(A) \cong {}^{A}/_{\ker\theta \cap A} = A/\ker\theta$ and hence

$$|G : A| = \frac{|G : \ker\theta|}{|A : \ker\theta|} = \frac{|K|}{|P|} = |K : P|$$

is *not* divisible by p. So if we take $H \in \mathrm{Syl}_p(A)$, H is also in $\mathrm{Syl}_p(G)$.
We have $\theta(H) \subseteq \theta(A) = P$ and by (a) $\theta(H)$ is a Sylow p-subgroup of K. Therefore $\theta(H) = P$, where H is a Sylow p-subgroup of G.

c) (a) and (b) together show that we have a surjective function

$$\widetilde{\theta} : \mathrm{Syl}_p(G) \to \mathrm{Syl}_p(K)$$
$$H \mapsto \theta(H)$$

Thus $|\mathrm{Syl}_p(K)| \leq |\mathrm{Syl}_p(G)|$ for every prime p.

6. $H \cap K$ is clearly a π-subgroup of K regardless of what HK is. If furthermore HK is a subgroup, H is also a Hall π-subgroup of HK. So no prime dividing $|K : H \cap K| = |HK : H|$ is in π.
Hence $H \cap K$ is a Hall π-subgroup of K.

7. a) Firstly we observe that if H and K are π-subgroups of G such that HK is a subgroup of G, then HK is necessarily a π-subgroup: Indeed, $|HK| = \frac{|H||K|}{|H \cap K|}$ so every prime p dividing $|HK|$ divides $|H||K|$; and since p is prime either $p \mid |H|$ or $p \mid |K|$. In any case $p \in \pi$.
A simple induction shows that if $H_1, \ldots, H_n$ are π-subgroups such that $H_1 \ldots H_n$ is a subgroup, $H_1 \ldots H_n$ is also a π-subgroup.
Now let X be the set of normal π-subgroups of G. $X \neq \emptyset$ since $1 \in X$ and X is finite since G is finite.
Then $N = \prod_{M \in X} M$ is a normal subgroup of G and by above observation N is a π-subgroup.
Our N satisfies the desired property.

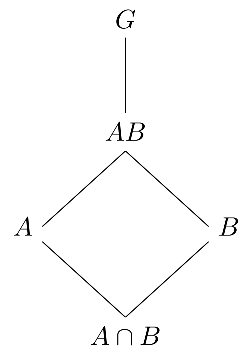
b) Let H be a Hall π-subgroup of G. Since $N \trianglelefteq G$, HN is a subgroup and by the observation in (a) HN is a π-subgroup. By 1B.6, $H \cap N$ is a Hall π-subgroup of N. But N is already a π-group itself; therefore $H \cap N = N$. Thus $N \subseteq H$.

c) By assumption the set $Y = \{\text{Hall } \pi\text{-subgroups of } G\}$ is nonempty. Let

$$V = \bigcap_{H \in Y} H$$

By (b), $N \subseteq V$.
On the other hand V is characteristic (it is canonically described), hence normal in G. Also V is clearly a π-subgroup. Thus by (a), $V \subseteq N$.

8. a) We first make an analogue observation to the one we did in 1B.7.a: Let A,B be normal in G such that G/A and G/B are π-groups.
$A \cap B$ is definitely normal in G. We claim that ${}^{G}/_{A \cap B}$ is also a π-group. Indeed, let p be a prime dividing $|{}^{G}/_{A \cap B}|$. Consider the lattice



Since $|{}^{G}/_{A \cap B}| = |G : A||A : A \cap B|$, we have two cases:
i) p divides $|G : A| = |G/A|$. G/A is a π-group, hence $p \in \pi$.
ii) p divides $|A : A \cap B| = |AB : B|$. Hence p divides $|G : B| = |G/B|$ and again $p \in \pi$.
This proves the claim. By a simple induction we see that if $A_1, \dots, A_n$ are normal in G such that G/A_i is a π-group for every i, then ${}^{G}/_{A_1 \cap \cdots \cap A_n}$ is also a π-group.
To answer the question, let $X = \{M \trianglelefteq G : G/M \text{ is a } \pi\text{-group}\}$. $X \neq \emptyset$ since $G \in X$ and X is finite since G is finite. Therefore by our observation, if we let

$$N = \bigcap_{M \in X} M,$$

G/N is a π-group.
Our N has the desired property.

b) Let H be the subgroup of G generated by elements that have order not divisible by any prime in π. H is canonically described, so H is characteristic in G.
We claim that G/H is a π-group:
Let p be a prime dividing $|G/H|$. By Cauchy's theorem, there exists $\overline{g} \in G/H$ of order p. So $g^p \in H$ but $g \notin H$.
Write $|g| = p^k n$ where $p \nmid n$. So there exist $a, b \in \mathbb{Z}$ such that $ap + bn = 1$. Then $g^{ap+bn} = g \notin H$. Since $g^p \in H$, we conclude that $g^n \notin H$.
Note that $|g^n| = p^k$. Since $g^n \notin H$, by definition of H $|g^n|$ has a prime divisor lying in π. Consequently we get $p \in \pi$.
So G/H is a π-group as we claimed. Thus by (a), $N \subseteq H$.
To see the reverse containment, let $g \in G$ be an element such that $|g|$ is not divisible by any prime in π. We will show that $g \in N$, since H is generated by such g's, this gives $H \subseteq N$.
Consider $\overline{g} \in G/N$. Suppose p is a prime dividing $|\overline{g}|$.
On one hand, $|\overline{g}|$ divides $|G/N|$. So $p \in \pi$ as G/N is a π-group.
On the other hand, $|\overline{g}|$ divides $|g|$. Therefore $p \notin \pi$.
A contradiction. So there is *no* prime dividing $|\overline{g}|$, which means $|\overline{g}| = 1$. Hence $\overline{g} = 1$, that is $g \in N$.

1C

1. Note that $H \trianglelefteq \mathbf{N}_G(H)$ and P is a Sylow p-subgroup of $\mathbf{N}_G(H)$ lying inside H. Therefore by the Frattini argument, $\mathbf{N}_G(H) = H\mathbf{N}_{\mathbf{N}_G(H)}(P) = H\mathbf{N}_G(P) = H$.

2. a) Since P is a p-subgroup of G, $P \subseteq S$ for some $S \in \mathrm{Syl}_p(G)$. So $P \subseteq S \cap H$.
But $S \cap H$ is a p-subgroup of H whereas $P \in \mathrm{Syl}_p(H)$. Thus $P = S \cap H$.

b) (a) gives a map

$$\begin{aligned} f : \mathrm{Syl}_p(H) &\to \mathrm{Syl}_p(G) \\ P &\mapsto S \text{ such that } S \cap H = P \end{aligned}$$

f is injective because $f(P) = f(Q)$ implies $P = f(P) \cap H = f(Q) \cap H = Q$.
Therefore $n_p(H) \leq n_p(G)$ (for every prime p).

3. a) Let $P \in \mathrm{Syl}_p(G)$. Every element of P has order equal to a power of p. Hence $P \subseteq X$.
P was arbitrary above, so

$$\bigcup_{P \in \mathrm{Syl}_p(G)} P \subseteq X$$

For the reverse containment, let $g \in X$. That is, $|g|$ is a power of p. So $\langle g \rangle$ is a p-subgroup of G, as a result $\langle g \rangle \subseteq P$ for some $P \in \mathrm{Syl}_p(G)$. Thus $g \in \bigcup_{P \in \mathrm{Syl}_p(G)} P$, and we are done.

b) Let $S \in \mathrm{Syl}_p(G)$. S acts on X by conjugation. Let X_0 be the set of fixed points of this action. As S is a p-group, we have

$$|X| \equiv |X_0| \pmod p$$

Note that X_0 is simply the set of elements in X that commute with every element of S. That is,

$$\begin{aligned} X_0 &= X \cap \mathbf{C}_G(S) \\ &= \bigcup_{P \in \mathrm{Syl}_p(G)} [P \cap \mathbf{C}_G(S)] \\ &= \bigcup_{P \in \mathrm{Syl}_p(G)} \mathbf{C}_P(S) \end{aligned}$$

We claim that $\mathbf{C}_P(S) \subseteq S$ for every $P \in \mathrm{Syl}_p(G)$.
Indeed, since $\mathbf{C}_P(S)$ and S commute elementwise, $\mathbf{C}_P(S)S$ is a subgroup of G. But $\mathbf{C}_P(S)$ is a p-subgroup, so by 1B.1.a our claim follows.
Furthermore we have $\mathbf{C}_P(S) \subseteq \mathbf{Z}(S)$ for every $P \in \mathrm{Syl}_p(G)$, as $\mathbf{C}_P(S)$ commutes with S and $\mathbf{C}_P(S) \subseteq S$.
Thus $X_0 \subseteq \mathbf{Z}(S)$. Also $\mathbf{Z}(S) = \mathbf{C}_S(S) \subseteq X_0$, so $X_0 = \mathbf{Z}(S)$. Now as $p \mid |G|$, S is nontrivial. Nontrivial p-groups have nontrivial centers[1], so p divides $|\mathbf{Z}(S)|$.
Consequently $|X| \equiv |\mathbf{Z}(S)| \equiv 0 \pmod p$: p divides $|X|$.

4. n_2 divides 15, so $n_2 \in \{1, 3, 5, 15\}$. Let $P \in \mathrm{Syl}_2(G)$. We argue case by case:
i) $n_2 = 1$. Then P is normal in G. Let $Q \in \mathrm{Syl}_5(G)$. PQ is a subgroup and $|PQ| = 40$, so $|G : PQ| = 3$.
ii) $n_2 = 3$ or 5. Then $n_2 = |G : \mathbf{N}_G(P)|$ is 3 or 5.
iii) $n_2 = 15$.[2] Let $S, T \in \mathrm{Syl}_2(G)$ with $S \neq T$ be such that $|S \cap T|$ is as large as possible. Note that $|S : S \cap T|$ is wither 2,4 or 8.
$15 = n_2 \equiv 1 \pmod{|S : S \cap T|}$ by Theorem 1.16. We see that $|S : S \cap T|$ must be 2. Let $D = S \cap T$.
$|S : D| = 2$ is the smallest prime dividing $|S| = 8$, so $D \trianglelefteq S$. Similarly $D \trianglelefteq T$.
Therefore $S, T \subseteq \mathbf{N}_G(D)$. Since $S \neq T$, $\mathbf{N}_G(D)$ strictly contains S. So $|G : \mathbf{N}_G(D)|$ is either 1, 3 or 5. If it is 3 or 5, we are done.
So assume it is 1. Then $D \trianglelefteq G$. Consider the factor group G/D, noting that $|G/D| = 30$. It is easy to see that $n_5(G/D) \in \{1, 6\}$.
If $n_5(G/D) = 1$, the subgroup $H/D \in \mathrm{Syl}_5(G/D)$ is normal in G/D, therefore $D \subseteq H \trianglelefteq G$ and $|H| = |H/D||D| = 5 \cdot 4 = 20$.
As H is normal, HS is a subgroup. To compute the order of HS, first note that $D \subseteq H \cap S \subseteq S$ and $|S : D| = 2$; so $H \cap S$ is either D or S. But $H \cap S = S$ implies $S \subseteq H$, contradicting Lagrange's

[1]According to Isaacs we are 'cheating' here since we use a result that is proven in the next section, Theorem 1.19. I would appreciate a 'non-cheating' argument.
[2]I think there should be a shorter argument dealing with this case.

theorem. Thus $H \cap S = D$ and

$$|HS| = \frac{|H||S|}{|D|} = \frac{20 \cdot 8}{4} = 40$$

$|G : HS| = 3$ and we are done.
The remaining case is $n_5(G/D) = 6$. Then G/D has $6 \cdot 4 = 24$ elements of order 5.
By Sylow theory $n_3(G/D) \in \{1, 10\}$. $n_3(G/D)$ cannot be 10 since we have at most $(30 - 1) - 24 = 5$ elements of order 3 in G/D.
Thus $n_3(G/D) = 1$. So $K/D \in \mathrm{Syl}_3(G/D)$ is normal in G/D. Hence $D \subseteq K \trianglelefteq G$ and $|K| = 12$.
KS is a subgroup. Similar to above we have $D \subseteq K \cap S \subseteq S$ but $K \cap S \neq S$ by Lagrange's theorem. Thus $D = K \cap S$ and

$$|KS| = \frac{|K||S|}{|D|} = \frac{12 \cdot 8}{4} = 24$$

$|G : KS| = 5$, done.

5. Although it is not excluded in the text, the assertion of the question is wrong for $p = 2$. So we assume p is an odd prime.
Since p is odd, p-cycles are inside A_{p+1}.
We observe that the highest power of p dividing $|A_{p+1}| = \frac{(p+1)!}{2}$ is 1: Indeed, $\frac{p+1}{2}$ is an integer since p is odd so we can factor out $|A_{p+1}|$ as

$$|A_{p+1}| = \frac{p+1}{2} \cdot p \cdot (p-1) \dots 1$$

Note that $p > 1$, $p > 2$, … , $p > p-1$ and $p > \frac{p+1}{2}$. In particular p does not divide any of $1, 2, \dots, p-1$ and $\frac{p+1}{2}$. Thus p, being a prime, does not divide $\frac{|A_{p+1}|}{p}$ (observation finito).
We conclude that the subgroups generated by p-cycles are the Sylow p-subgroups of A_{p+1}. Total number of p-cycles in S_{p+1} (hence in A_{p+1}) is $(p+1)(p-1)!$. Every Sylow p-subgroup of A_{p+1} contains exactly $p-1$ p-cycles and every p-cycle is contained in exactly one Sylow p-subgroup (namely the one it generates), thus

$$n_p(A_{p+1}) = \frac{(p+1)(p-1)!}{p-1} = (p+1)(p-2)!$$

Therefore

$$|N_G(P)| = \frac{|A_{p+1}|}{|n_p|} = \frac{(p+1)!}{2} \cdot \frac{1}{(p+1)(p-2)!} = \frac{p(p-1)}{2}$$

6. a) Take $A \in \mathrm{Syl}_p(H)$. By 1C.2.a $A = Q \cap H$ for some $Q \in \mathrm{Syl}_p(G)$. Take $B \in \mathrm{Syl}_p(K)$. Again by 1C.2.a $B = S \cap H$ for some $S \in \mathrm{Syl}_p(G)$. $S = Q^g$ for some $g \in G$. Write $g = hk$ with $h \in H$ and $k \in K$. Then

$$B = Q^{hk} \cap K = Q^{hk} \cap K^k = (Q^h \cap K)^k$$

so $Q^h \cap K \in \mathrm{Syl}_p(K)$.
Also

$$Q^h \cap H = Q^h \cap H^h = (Q \cap H)^h = A^h \in \mathrm{Syl}_p(H)$$

Hence $P = Q^h \in \mathrm{Syl}_p(G)$ is the desired subgroup.

b)

$$|(P \cap H)(P \cap K)| = \frac{|P \cap H||P \cap K|}{|P \cap H \cap K|} = \frac{|H|_p |K|_p}{|P \cap H \cap K|}$$

where the p-subscript denote the p-part of a positive integer.
We also have $|P \cap H \cap K| \leq |H \cap K|_p$ since $P \cap H \cap K$ is a p-subgroup of $H \cap K$. Thus

$$|(P \cap H)(P \cap K)| \geq \frac{|H|_p |K|_p}{|H \cap K|_p} = \left(\frac{|H||K|}{|H \cap K|}\right)_p = |HK|_p = |G|_p$$

But as a set $(P \cap H)(P \cap K)$ is contained in P and $|P| = |G|_p$.
Therefore $(P \cap H)(P \cap K) = P$.

7. Suppose not, that is $\mathbf{N}_G(P) < G$ for $P \in \mathrm{Syl}_p(G)$. So there is a maximal subgroup M such that $\mathbf{N}_G(P) \subseteq M$. Since $P \in \mathrm{Syl}_p(G)$ and $P \subseteq M$, $P \in \mathrm{Syl}_p(M)$. Therefore $n_p(M) = |M : \mathbf{N}_M(P)| = |M : \mathbf{N}_G(P)|$.
Since $n_p(G) = |G : \mathbf{N}_G(P)| = |G : M| n_p(M)$ and both $n_p(G)$ and $n_p(M)$ are 1 modulo p, we get

$$|G : M| \equiv 1 \pmod{p}$$

By the assumptions $|G : M| = q$ is prime and $q \leq p$ whereas the above yields $p \mid q-1$. Since $q-1 \neq 0$, we get $p \leq q-1$, a contradiction.

8. P acts on $\Omega = \{\text{subgroups of G of order } p^a\}$ by conjugation. Let Ω_0 be the set of fixed points.
Let $Q \in \Omega_0$. Then P fixes Q by conjugation, that is $P \subseteq \mathbf{N}_G(Q)$. So PQ is a subgroup. By 1B.1.a $Q \subseteq P$. We conclude that

$$\Omega_0 = \{Q \trianglelefteq P : |Q| = p^a\}$$

P is a p-group, hence $|\Omega| \equiv |\Omega_0| \pmod{p}$.
P also acts on $\Lambda = \{\text{subgroups of P of order } p^a\}$ by conjugation. Note that the set of fixed points under this action is also Ω_0. Therefore $|\Lambda| \equiv |\Omega_0| \pmod{p}$. We get

$$|\Lambda| \equiv |\Omega| \pmod{p}$$

as desired.

1D

1. We showed in the solution of 1A.10 that

$$|G : P| \equiv |\mathbf{N}_G(P) : P| \pmod{p}$$

Since $P \subseteq \mathbf{N}_G(P) \subseteq H$ and $P \in \mathrm{Syl}_p(H)$, $|\mathbf{N}_G(P) : P|$ is not divisible by p. So we cancel it above and get

$$|G : \mathbf{N}_G(P)| \equiv 1 \pmod{p}$$

Furthermore,

$$|H : \mathbf{N}_G(P)| = n_p(H) \equiv 1 \pmod{p}$$

Thus $|G : H| \equiv 1 \mod p$.

2. Assume p divides $|H|$. We will show that p does not divide $|G : H|$.
Take $P \in \mathrm{Syl}_p(G)$, so p divides $|P|$. Letting $\Omega = \{\text{elements in } P \text{ of order } p\}$ and using (1A.8) we get $|\Omega| \equiv -1 \pmod{p}$.
Note that $\mathbf{N}_G(P)$ acts on Ω by conjugation. Let $x_1, \ldots x_n \in \Omega$ be representatives of distinct orbits of this action. Then

$$|\Omega| = \sum_{i=1}^{n} \left|\mathbf{N}_G(P) : \mathbf{C}_{\mathbf{N}_G(P)}(x_i)\right|$$

Since x_i's are in H, using the given assumption we have

$$\mathbf{C}_{\mathbf{N}_G(P)}(x_i) = \mathbf{C}_G(x_i) \cap \mathbf{N}_G(P) \subseteq H \cap \mathbf{N}_G(P) = \mathbf{N}_H(P)$$

for every i. In particular $|\mathbf{N}_G(P) : \mathbf{N}_H(P)|$ divides $|\mathbf{N}_G(P) : \mathbf{C}_{\mathbf{N}_G(P)}(x_i)|$ for every i, thus $|\mathbf{N}_G(P) : \mathbf{N}_H(P)|$ divides $|\Omega|$.
Then since $|\Omega| \equiv -1 \pmod{p}$, $|\mathbf{N}_G(P) : \mathbf{N}_H(P)|$ is not divisible by p.
$|\mathbf{N}_H(P) : P|$ is also not divisible by p as $P \in \mathrm{Syl}_p(H)$. p is a prime, therefore p does not divide $|\mathbf{N}_G(P) : \mathbf{N}_H(P)||\mathbf{N}_H(P) : P| = |\mathbf{N}_G(P) : P|$.
P is a p-subgroup of G, so by (1A.10), p does not divide $|G : P|$. Therefore p does not divide $|G : H|$.

3. a) Let $g \in \mathbf{N}_G(K)$. Then $1 < K = K \cap K^g \subseteq H \cap H^g$. Hence by assumption $g \in H$.

b) Fix a prime p.
By (a), for every $x \in H$ with $|x| = p$ we have

$$\mathbf{C}_G(x) = \mathbf{N}_G(\langle x \rangle) \subseteq H$$

since $1 < \langle x \rangle \subseteq H$.
Therefore the hypothesis of the problem 1D.2 is satisfied. So p cannot divide both $|H|$ and $|G:H|$.
The prime p was arbitrary above. It follows that $|H|$ and $|G:H|$ cannot have a common prime in their factorizations. That is, $|H|$ and $|G:H|$ are coprime.

4. Assume H is a Frobenius complement in G. For $h \in H - \{1\}$, take $n \in \mathbf{C}_N(h)$. Then since $1 \neq h = h^n$ is in $H \cap H^n$, we must have $n \in H$. But then $n \in H \cap N = 1$, so $n = 1$.
Conversely, assume $\mathbf{C}_N(h) = 1$ for all $h \neq 1$ in H. Assuming $H \cap H^g \neq 1$, we will show $g \in H$.
Write $g = hn$ with $h \in H$ and $n \in N$. So $1 \neq H \cap H^{hn} = H \cap H^n$. So there exists $x \neq 1$ in H such that $x^n \in H$.
Note that $x^{-1}x^n = x^{-1}n^{-1}xn \in N$ since N is normal.
But then $x^{-1}x^n \in N \cap H = 1$, so $x = x^n$. That is, $n \in \mathbf{C}_N(x) = 1$. Thus $g = hn = h \in H$.

5. Let's observe what Isaacs wants us to observe. If P is a p-subgroup of $H \cap H^g$, $\mathbf{N}_G(P) \subseteq H$ by hypothesis. Also, since $P^{g^{-1}}$ is also a p-subgroup of H, $[\mathbf{N}_G(P)]^{g^{-1}} = \mathbf{N}_G(P^{g^{-1}}) \subseteq H$, meaning $\mathbf{N}_G(P) \subseteq H^g$. Thus $\mathbf{N}_G(P) \subseteq H \cap H^g$.
Assuming $H \cap H^g \neq 1$, we show that $g \in H$:
There is a nontrivial Sylow subgroup Q of $H \cap H^g$. Say $Q \in \mathrm{Syl}_p(H \cap H^g)$. Then $\mathbf{N}_G(Q) \subseteq H \cap H^g$ by the above observation.
We claim that $Q \in \mathrm{Syl}_p(H)$. If not, p divides $|H : Q|$. By 1A.10, p divides $|\mathbf{N}_H(Q) : Q|$.
But $\mathbf{N}_H(Q) = \mathbf{N}_G(Q) \subseteq H \cap H^g$, which in turn implies that $|H \cap H^g : Q|$ is divisible by p, contradicting $Q \in \mathrm{Syl}_p(H \cap H^g)$. Our claim is indeed true.
Now observe that $Q^{g^{-1}} \subseteq H$, so $Q^{g^{-1}}$ is also a Sylow p-subgroup of H. Thus there exists $h \in H$ such that $Q^{g^{-1}h} = Q$. Then $g^{-1}h \in \mathbf{N}_G(Q) \subseteq H$, so $g \in H$.

6. Subgroups of prime index are always maximal by Lagrange's theorem, regardless of nilpotence.
For the converse, let M be a maximal subgroup of a nilpotent group G. Then M is normal in G.
Therefore G/M has only two subgroups (M/M and G/M), and the only groups with this property are cyclic groups of prime order. Thus $|G : M| = |G/M| = p$ for some prime p.

7. Let $g \in \Phi(G)$. Suppose $\langle X \cup \{g\} \rangle = G$ but $\langle X \rangle \neq G$. Then $\langle X \rangle$ is contained in a maximal subgroup M. But $g \in \Phi(G)$ is also in M, so $X \cup \{g\} \subseteq M$ hence $\langle X \cup \{g\} \rangle \neq G$, a contradiction.
Conversely, let $g \in G$ be a "useless" element.
For any maximal subgroup M of G, $\langle M \rangle = M \neq G$. So by "uselessness" of g, $\langle M \cup \{g\} \rangle \neq G$.
Since $M \subseteq \langle M \cup \{g\} \rangle \subsetneq G$, it follows by maximality of M that $g \in M$.
Thus g is inside every maximal subgroup: $g \in \Phi(G)$.

8. a) In 1D.6 we showed that G/M is cyclic, hence abelian for every maximal subgroup M. Therefore $G' \subseteq M$ for every maximal M. Hence $G' \subseteq \Phi(G)$, so $G/\Phi(G)$ is abelian.

b) By 1D.6 $|G : M|$ is a prime number for every maximal subgroup M. Since G is a p-group, $|G : M| = p$ for every maximal subgroup M. Therefore for every $g \in G$, $g^p \in \bigcap_{M\text{-maximal}} M = \Phi(G)$, that is $(\overline{g})^p = 1$ in $G/\Phi(G)$. It follows that $G/\Phi(G)$ is elementary abelian.

9. Contrapositively, we show that if $|P : \Phi(P)| < p^2$, P is cyclic. Certainly $\Phi(P) < P$, so the only possibility is $|P : \Phi(P)| = p$. Then $\Phi(P)$ itself is a maximal subgroup of P, it follows that $\Phi(P)$ is the *unique* maximal subgroup of P.
Take $x \in P - \Phi(P)$. Then $\langle x \rangle$ must equal P, because otherwise $\langle x \rangle$ is contained in a maximal subgroup, which is necessarily $\Phi(P)$; a contradiction. So $P = \langle x \rangle$ is cyclic.
In particular if $|P| = p^2$, either P is cyclic or $|P : \Phi(P)| \geq p^2 = |P|$.
In the latter case, we get $\Phi(P) = 1$. Then by (8), $P \cong P/\Phi(P)$ is elementary abelian.

10. Clearly $A \subseteq \mathbf{C}_P(A)$ since A is abelian.
Suppose $C = \mathbf{C}_P(A) > A$. Apply Lemma 1.23 to A and C. (both A and C are normal in P) to get $B \trianglelefteq P$ such that $A \subseteq B \subseteq C$ and $|B : A| = p$.
Here, A and B commute elementwise hence $A \subseteq \mathbf{Z}(B)$. Then $|B : \mathbf{Z}(B)|$ divides $|B : A| = p$, i.e. $|B : \mathbf{Z}(B)|$ is 1 or p.
But the quotient group formed by dividing a group to its center is never cyclic unless it is trivial, so $|B : \mathbf{Z}(B)| \neq p$.
Thus $B = \mathbf{Z}(B)$; B is abelian. But B is also normal and strictly contains A, contradicting A being a maximal abelian normal subgroup.
As a result, our initial assumption is wrong, so $A = \mathbf{C}_P(A)$.
Now P acts on A by conjugation (as $A \trianglelefteq P$) and the identity element is a fixed point of the action. Therefore P also acts on $A - \{1\}$ by conjugation.
This gives us a homomorphism $\varphi : P \to \mathrm{Sym}\,(A - \{1\})$ with kernel

$$\ker\varphi = \mathbf{C}_P(A - \{1\}) = \mathbf{C}_P(A) = A$$

By the first isomorphism theorem, $|P : A|$ divides $|\mathrm{Sym}(A - \{1\})| = (|A| - 1)!$
(so $|P|$ divides $|A|!$)

11. $|G|$ is the least common multiple of the orders of (nontrivial) Sylow subgroups of G. So it suffices to check that for every prime p, $|P|$ divides $n!$ where $P \in \mathrm{Syl}_p(G)$.
Indeed, let p be a prime and let $P \in \mathrm{Syl}_p(G)$. There exists a maximal abelian normal subgroup A of P (P is finite, after all). Let $m = |A|$. By (10), $|P|$ divides $m!$.
Now A is an abelian subgroup of G, therefore $m \leq n$. Thus $|P|$ divides $n!$.

12. Well, we did this in 1A.8.

13. G/Z has a central series, say (denoting G/Z with $\overline{G}$)

$$\overline{1} = \overline{N_0} \subseteq \overline{N_1} \subseteq \cdots \subseteq \overline{N_r} = \overline{G} \tag{1}$$

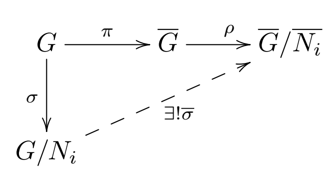
is one.
We know that $\overline{N_i}$'s are of the form N_i/Z where $N_i \trianglelefteq G$. Consider the series

$$Z = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_r = G \tag{2}$$

The third isomorphism theorem basically seals the deal here, but it has to be invoked two times and one must somehow make sure that the isomorphisms used at these two instances are the "same".
So we work in a more cumbersome way to leave no doubts.
Fix $i \in \{0, 1, \ldots, r\}$.
Consider the natural projections

$$\pi : G \to G/Z = \overline{G}$$
$$\rho : \overline{G} \to \overline{G}/\overline{N_i}$$
$$\sigma : G \to G/N_i$$

The composition $\rho \circ \pi : G \to \overline{G}/\overline{N_i}$ is surjective and has kernel N_i.
Therefore there is a *unique isomorphism* $\overline{\sigma} : G/N_i \to \overline{G}/\overline{N_i}$ making the diagram



commute. Since (1) is a central series, we have $\overline{N_{i+1}}\,/\overline{N_i} \subseteq \mathbf{Z}\left(\overline{G}/\overline{N_i}\right)$. Rewriting this inclusion using our natural projections and the above commutative diagram gives

$$\begin{aligned} \pi(N_{i+1})\,/\overline{N_i} &\subseteq \mathbf{Z}\left(\pi(G)\,/\overline{N_i}\right) \\ (\rho\circ\pi)(N_{i+1}) &\subseteq \mathbf{Z}\left((\rho\circ\pi)(G)\right) \\ (\overline{\sigma}\circ\sigma)(N_{i+1}) &\subseteq \mathbf{Z}\left((\overline{\sigma}\circ\sigma)(G)\right) \\ \overline{\sigma}\left(N_{i+1}\,/N_i\right) &\subseteq \mathbf{Z}\left(\overline{\sigma}\left(G/N_i\right)\right) = \overline{\sigma}\left(\mathbf{Z}\left(G/N_i\right)\right) \end{aligned}$$

where the last equality holds because $\overline{\sigma}$ is an isomorphism. Again as $\overline{\sigma}$ is an isomorphism, we can cancel it in the last inclusion above and get

$$N_{i+1}\,/N_i \subseteq \mathbf{Z}(G/N_i)$$

This almost proves that (2) is a central series; but no, (2) does not start with 1. We simply add 1 to get

$$1 \subseteq Z = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_r = G$$

The only remaining thing to show that this is a central series is $Z \subseteq \mathbf{Z}(G)$, and this is given as an assumption. Thus G is nilpotent.

14. We prove a more general statement in 1D.15.

15. Let P be a Sylow subgroup of N. We will show that $P \trianglelefteq N$.
By 1B.5.a, surjective homomorphisms map Sylow subgroups to Sylow subgroups.
Thus $P\Phi(G)\,/\Phi(G)$ is a Sylow subgroup of $N\,/\Phi(G)$, hence by nilpotence $P\Phi(G)\,/\Phi(G)$ is normal in $N\,/\Phi(G)$.
Normal Sylow subgroups are characteristic, so

$$P\Phi(G)\,/\Phi(G) \text{ char } N\,/\Phi(G) \trianglelefteq G\,/\Phi(G)$$

Therefore $P\Phi(G)\,/\Phi(G) \trianglelefteq G\,/\Phi(G)$, hence $P\Phi(G) \trianglelefteq G$.
Since $P \subseteq P\Phi(G) \subseteq N$, P is also a Sylow subgroup of $P\Phi(G)$. By Frattini argument, $N_G(P)(P\Phi(G)) = G$. So $N_G(P)\Phi(G) = G$.
This implies $N_G(P) = G$, because otherwise $N_G(P)$ would be contained in a maximal subgroup M and we would obtain $G = N_G(P)\Phi(G) \subseteq M$, a contradiction.
Thus $P \trianglelefteq G$, in particular $P \trianglelefteq N$.

16. Since $\Phi(N)$ char $N \trianglelefteq G$, $\Phi(N) \trianglelefteq G$.
Suppose M is a maximal subgroup that does not contain $\Phi(N)$. Then $\Phi(N)M$ is a subgroup strictly containing M, hence $\Phi(N)M = G$.
We have $N = G \cap N = \Phi(N)M \cap N = \Phi(N)(M \cap N)$, where the last equality is by Dedekind's lemma.[3]
Then necessarily we have $N = M \cap N$. So $N \subseteq M$, contradicting $\Phi(N) \nsubseteq M$.
Consequently every maximal subgroup of G contains $\Phi(N)$; so $\Phi(N) \subseteq \Phi(G)$.

17. N is nilpotent, so $N\,/\Phi(N)$ is abelian by 1D.8. So $N' \subseteq \Phi(N)$.
Let M be a maximal subgroup of G; we will show that $M \trianglelefteq G$. By 1D.16 $\Phi(N) \subseteq M$. Hence $N' \subseteq M$, so M/N' is a maximal subgroup of G/N'. G/N' is nilpotent, so $M/N' \trianglelefteq G/N'$. Thus $M \trianglelefteq G$.

18. Being abelian, $\mathbf{Z}(G)$ is nilpotent. Also $\mathbf{Z}(G) \trianglelefteq G$, so by Lemma 1.28 $\mathbf{Z}(G) \subseteq \mathbf{F}(G)$.
$\mathbf{F}(G)/\mathbf{Z}(G)$ is nilpotent as $\mathbf{F}(G)$ is nilpotent. Also $\mathbf{F}(G)/\mathbf{Z}(G) \trianglelefteq G/\mathbf{Z}(G)$.
We will show that every normal nilpotent subgroup of $G/\mathbf{Z}(G)$ is contained in $\mathbf{F}(G)/\mathbf{Z}(G)$, which implies $\mathbf{F}\left(G/\mathbf{Z}(G)\right) = \mathbf{F}(G)/\mathbf{Z}(G)$.
Indeed, let $N/\mathbf{Z}(G)$ be a normal nilpotent subgroup of $G/\mathbf{Z}(G)$.
Note that $\mathbf{Z}(G) \subseteq \mathbf{Z}(N)$, so by 1D.13 N is nilpotent. Also $N \trianglelefteq G$, hence $N \subseteq \mathbf{F}(G)$.
Therefore $N/\mathbf{Z}(G) \subseteq \mathbf{F}(G)/\mathbf{Z}(G)$.

[3] It is located in the appendix as Lemma X.3 .

19. I couldn't solve this problem.

1E

1. $n_q(G)$ (shortly n_q) divides p^2 so there are three cases to consider:
i) $n_q = 1$. This is what we want.
ii) $n_q = p$. Then $p \equiv 1 \pmod q$, but this is impossible because $1 < p < q$.
iii) $n_q = p^2$. Then $p^2 \equiv 1 \pmod q$, so either $p \equiv 1 \pmod q$ or $p \equiv -1 \pmod q$. The former is outruled in (ii), so $p \equiv -1 \pmod q$, that is $q \mid p+1$.
Then we get $p < q \le p+1$ which means $q = p+1$. The only primes satisfying this are $p = 2$, $q = 3$ and in this case $|G| = 36$.

2. n_r divides pq, so there are three cases to consider:
i) $n_r = 1$. Good.
ii) $n_r = p$ or q. But then $p \equiv 1 \pmod r$ or $q \equiv 1 \pmod r$, both are impossible because $1 < p, q < r$.
iii) $n_r = pq$. Then the number of elements in G of order r is $pq(r-1) = |G| - pq$.
Now we consider n_q. Since $1 < p < q$, $n_q \neq p$ (as $n_q \equiv 1 \pmod q$).
Suppose $n_q \ge r$. Then the number of elements in G of order q is $r(q-1)$. Combining these with the elements of order r, we get $|G| - pq + rq - r$ elements in G. Therefore $pq - rq + r \ge 0$.
So $r \ge q(r-p) \ge (p+1)(r-p) = pr - p^2 + r - p$. This yields $p + 1 \ge r$, a contradiction.
So we showed that $n_q < r$ and $n_q \neq p$. Since n_q divides pr, necessarily $n_q = 1$. Hence $Q \in \mathrm{Syl}_q(G)$ is normal.
Now G/Q is a group of order pr, where $p < r$. By Theorem 1.30, $n_r(G/Q) = 1$. So $A/Q \in \mathrm{Syl}_r(G/Q)$ is normal in G/Q. So $A \trianglelefteq G$ and $|A| = qr$.
Take $R \in \mathrm{Syl}_r(A)$. Again by Theorem 1.30, $R \trianglelefteq A$. Normal Sylow subgroups are characteristic, so R char $A \trianglelefteq G$. Hence $R \trianglelefteq G$. But $|R| = r$ so $R \in \mathrm{Syl}_r(G)$, contradicting $n_r = pq$.

3. Suppose G is simple, where $|G| = 315$.
Then $n_3 \in \{5, 7, 35\}$.
Take $S, T \in \mathrm{Syl}_3(G)$ with $S \neq T$ such that $S \cap T$ is as large as possible. $|S : S \cap T|$ is 3 or 9. Since $n_3 \equiv 1 \pmod{|S : S \cap T|}$ and none of $5, 7, 35$ are 1 modulo 9, so $|S : S \cap T| = 3$.
Let $D = S \cap T$, we see that $D \trianglelefteq S$, $D \trianglelefteq T$.
So $S, T \subseteq \mathbf{N}_G(D)$. Say $N = \mathbf{N}_G(D)$. Since $S \neq T$, there are three possibilities for $|N|$:
i) $|N| = 3^2 \cdot 5$. But then we see that $n_3(N) = 1$, contradicting $S, T \subseteq N$ with $S \neq T$.
ii) $|N| = 3^2 \cdot 7$. Then $|G : N| = 5$ but $|G|$ does not divide $5! = 120$, contradicting the $n!$-theorem.
iii) $|N| = 3^2 \cdot 5 \cdot 7$. That is $N = G$, so $D \trianglelefteq G$, a contradiction.

4. Suppose G is simple. Then $n_3 \in \{2, 4, 8, 16\}$. Let $P \in \mathrm{Syl}_3(G)$. Since $n_3 = |G : \mathbf{N}_G(P)|$, by $n!$-theorem $n_3 \neq 2$, $n_3 \neq 4$.
Now take $S, T \in \mathrm{Syl}_3(G)$ with $S \neq T$ such that $S \cap T$ is as large as possible. $|S : S \cap T|$ is 3 or 9.
Since $n_3 \equiv 1 \pmod{|S : S \cap T|}$ it follows that $|S : S \cap T| = 3$ and $n_3 = 16$.
Let $D = S \cap T$. We see as usual that $S, T \subseteq \mathbf{N}_G(D)$.
Let $N = \mathbf{N}_G(D)$. By $n!$-theorem $|G : N|$ cannot be 2 or 4. $S < N$, so $|G : N|$ is not 16 either.
If $|G : N| = 1$ $D \trianglelefteq G$, a contradiction.
The only remaining case is $|G : N| = 8$. So $|N| = 2 \cdot 3^2$, but then $n_3(N) = 1$, contradicting $S, T \subseteq N$.

5. Suppose G is simple. By Sylow theory we see that $n_7 = 8$. That is for $P \in \mathrm{Syl}_7(G)$, $|G : \mathbf{N}_G(P)| = 8$.
Since G is simple there is an injective homomorphism $\iota : G \to S_8$.
Here $\iota(G) \subseteq A_8$; because otherwise $\iota(G) \subseteq A_8$ is an index 2 subgroup of $\iota(G) \cong G$, contradicting the simplicity of G.
So we can see G as a subgroup of A_8. By order considerations, we have
$P \in \mathrm{Syl}_7(A_8)$. By (1C.5), $|\mathbf{N}_{A_8}(P)| = \frac{7 \cdot 6}{2} = 21$.
But $\mathbf{N}_G(P)$ is contained in $\mathbf{N}_{A_8}(P)$ and $|\mathbf{N}_G(P)| = \frac{|G|}{8} = 42$, a contradiction.

6. Suppose G is simple. By basic Sylow theory we see that $n_3 \in \{4, 10\}$. Since G is simple and $|G| = 180$, n!-theorem forces $n_3 = 10$.
Take two distinct Sylow 3-subgroups S and T such that $S \cap T$ is as large as possible. $|S : S \cap T|$ is 3 or 9, and $n_3 \equiv 1 \pmod{|S : S \cap T|}$. Hence there are two cases:
i) $|S \cap T| = 1$.
So every pair of the 10 Sylow 3-subgroups intersect trivially.
So we get $10(9 - 1) = 80$ nonidentity elements from the Sylow 3-subgroups.
Again by Sylow theory $n_5 \in \{6, 36\}$.
If $n_5 = 6$, (similar to the previous question) we get an embedding $G \hookrightarrow A_6$. But A_6 is simple, whereas $|A_6 : G| = 360/180 = 2$, a contradiction.
So $n_5 = 36$. Hence we get $36(5 - 1) = 144$ nonidentity elements from the Sylow 5-subgroups.
$144 + 80$ exceeds $|G|$, contradiction.
ii) $|S \cap T| = 3$.
Letting $D = S \cap T$, we get $S, T \subseteq \mathbf{N}_G(D)$. Let $N = \mathbf{N}_G(D)$.
$|G : N| \in \{1, 2, 5, 10\}$ since $S < N$.
$|G : N|$ being 2, 4 or 5 contradicts n!-theorem.
$|G : N| = 1$ gives $D \trianglelefteq G$. Contradiction.
If $|G : N| = 10$, $|N| = 18$ but then $n_3(N) = 1$, contradicting $S, T \subseteq N$.

7. Suppose G is simple. $n_2 \in \{3, 5, 15\}$ by Sylow theory. By n!-theorem we obtain $n_2 = 15$ (240 does not divide 3! and 5!).
Take two distinct Sylow 2-subgroups S and T such that $S \cap T$ is as large as possible. $|S : S \cap T| \in \{2, 4, 8, 16\}$ and $15 = n_2 \equiv 1 \pmod{|S : S \cap T|}$, so we get $|S : S \cap T| = 2$. Letting $D = S \cap T$, we see that $S, T \subseteq \mathbf{N}_G(D)$. Let $N = \mathbf{N}_G(D)$.
Since $S < N$, $|G : N| \in \{1, 3, 5\}$. By n!-theorem $|G : N|$ can't be 3 or 5. So $|G : N| = 1$ but then $D \trianglelefteq G$, contradiction.

8. Suppose G is simple. By Sylow theory and n!-theorem we see that $n_3 \in \{7, 28\}$ and $n_7 = 36$.
Take two distinct Sylow 3-subgroups S and T such that $S \cap T$ is as large as possible. $|S : S \cap T|$ is 3 or 9. Noting that $n_3 \equiv 1 \pmod{|S : S \cap T|}$, we consider both cases:
i) $|S : S \cap T| = 9$. Then $n_3 = 28$. So every pair of the 28 Sylow 3-subgroups intersect trivially, therefore we get $28(9 - 1) = 224$ nonidentity elements out of them. But we also have $36(7 - 1) = 216$ nonidentity elements from the Sylow 7-subgroups. $224 + 216$ exceed $|G|$, contradiction.
ii) $|S : S \cap T| = 3$. Letting $D = S \cap T$ and $N = \mathbf{N}_G(D)$, we see that $S, T \subseteq N$. D cannot be normal as G is simple and N strictly contains S, hence using also the n!-theorem we obtain $|G : N| \in \{7, 14\}$.
If $|G : N| = 14$, $|N| = 18$. But then $n_3(N) = 1$, contradicting $S, T \subseteq N$.
Hence $|G : N| = 7$. So $|N| = 36$. Basic Sylow theory and $n_3(N) \geq 2$ implies $n_3(N) = 4$. Observe that since $D \trianglelefteq N$ and $|D| = 3$, every pair of distinct Sylow 3-subgroups in N intersect at D. Therefore there are $8 + 6 + 6 + 6 = 26$ nonidentity elements coming from the Sylow 3-subgroups of N.
Note that $\mathrm{Syl}_3(N) \subsetneq \mathrm{Syl}_3(G)$. Take a Sylow 3-subgroup U of G that is not contained in N. Since $|U \cap N|$ is at most 3, we get 6 new elements. Summing up, we have $26 + 6 = 32$ nonidentity elements coming from Sylow 3-subgroups. As noted above, we have 216 nonidentity elements from Sylow 7-subgroups. But this leaves only $252 - (216 + 32) = 3$ elements, which is not enough for a Sylow 2-subgroup to fit. Contradiction.

1F

1. On the one hand, $m^{-1}n^{-1}mn = m^{-1}m^n \in M$ since M is normal. On the other hand, $m^{-1}n^{-1}mn = (n^{-1})^{m^{-1}}n \in N$ since N is normal. Thus $m^{-1}n^{-1}mn \in M \cap N = 1$, that is $mn = nm$.

2. Pick $S, T \in \mathrm{Syl}_p(G)$ as in Theorem 1.38.
Since $\mathbf{Z}(S) \cap \mathbf{Z}(T) \subseteq \mathbf{Z}(S)$, $\mathbf{Z}(S) \cap \mathbf{Z}(T) \trianglelefteq S$. Similarly $\mathbf{Z}(S) \cap \mathbf{Z}(T) \trianglelefteq T$. But $\mathbf{O}_p(G) = 1$ is the largest subgroup of $S \cap T$ that is normal in both S and T (by Theorem 1.38), hence $\mathbf{Z}(S) \cap \mathbf{Z}(T) = 1$.

3. I couldn't solve this problem.

1G

1. We already know that $|G:M| \leq |G:A|^2$, where M is the Chermak-Delgado subgroup, by Theorem 1.41.
M is characteristic and abelian, therefore the hypothesis of the problem forces $|G:M| = |G:A|^2$.
Therefore every inequality used in the proof of Theorem 1.41 must degenerate to an equality.
Hence, parsing the proof, we get:

(1) $m_G(M) = m_G(A)$

(2) $|\mathbf{C}_G(A)| = |A|$

(3) $\left|\frac{G}{\mathbf{C}_G(M)}\right| = 1$

(1) means A is in $\mathcal{L}(G)$. (2) means $A = \mathbf{C}_G(A)$.
(3) means $\mathbf{C}_G(M) = G$, that is $M \subseteq \mathbf{Z}(G)$. We also have $\mathbf{Z}(G) \subseteq M$ by Corollary 1.45, so $M = \mathbf{Z}(G)$.
Thus $|G:\mathbf{Z}(G)| = |G:M| = |G:A|^2$.

2. Let $X = \{L \in \mathcal{L}(G) : H \subseteq L < G\}$. H is in X, so $X \neq \emptyset$. Since X is a finite set, it has a maximal element K (with respect to inclusion). We claim that for every $g \in G$, $H^g \subseteq K$.
Suppose not, i.e. there exists $g \in G$ such that $H^g \nsubseteq K$.
Now since conjugation by g is an automorphism of G, $H^g \in \mathcal{L}(G)$. By Theorem 1.44, H^gK is a subgroup in the lattice $\mathcal{L}(G)$, and $H \subseteq K \subsetneq H^gK$. The maximality of K in X forces $H^gK = G$.
Then we can write the element g^{-1} as $g^{-1} = h^gk$ for some $h \in H$, $k \in K$. So $g^{-1} = g^{-1}hgk$, hence $hgk = 1$. But $h \in H \subseteq K$ and $k \in K$, thus $g \in K$.
Therefore $H^g \subseteq K$, giving $K = G:$ a contradiction.
As a result, our claim holds. That is, for every $g \in G$, $H^g \subseteq K$. Equivalently for every $g \in G$, $H \subseteq K^g$.
Hence $H \subseteq \bigcap_{g \in G} K^g = \mathrm{core}_G(K)$ and $\mathrm{core}_G(K)$ is a proper normal subgroup of G (as $K < G$).

3. If G is abelian, $|G| = |H||\mathbf{C}_G(H)| = |H||G|$, so $H = 1$.
So we may assume G is nonabelian.
Let M be the Chermak-Delgado subgroup of G. Then $M < G$ since M is abelian and G is nonabelian.
Then $M = 1$ since G is simple. Consequently $m_M(G) = |G| = m_H(G)$, so $H \in \mathcal{L}(G)$.
Assuming $H < G$, we will show $H = 1$. Indeed, by 1G.2 there is a normal subgroup N of G such that $H \subseteq N < G$. But G is simple, so $N = 1$. Thus $H = 1$.

4. Suppose there is no normal abelian subgroup N of G with $|G:N| < |G:A|^2$, to the contrary.
Since characteristic subgroups are normal, by 1G.1, $A = C_G(A) \in \mathcal{L}(G)$ and
$|G:\mathbf{Z}(G)| = |G:A|^2$.
Note that $\mathbf{Z}(G) \subseteq \mathbf{C}_G(A) = A$. So the set $X = \{B \in \mathcal{L}(G) : \mathbf{Z}(G) \subseteq B \text{ and } B \text{ is abelian}\}$ is not empty ($A \in X$). X is a finite set. By Theorem 1.44, $\widetilde{A} = \prod_{B \in X} B$ is a subgroup of G in $\mathcal{L}(G)$.
Observe that $\widetilde{A}$ is characteristic in G (The set X, hence $\widetilde{A}$ is canonically described). Also as a product of abelian groups, $\widetilde{A}$ is abelian. There are two cases:
i) $\widetilde{A} > \mathbf{Z}(G)$. Then $|G:\widetilde{A}| < |G:\mathbf{Z}(G)| = |G:A|^2$, contradicting our very first assumption.
ii) $\widetilde{A} = \mathbf{Z}(G)$. But $\mathbf{Z}(G) \subseteq A \subseteq \widetilde{A}$, so $A = \mathbf{Z}(G)$.
Hence A is a normal abelian subgroup and $|G:A| > 1$ since G is nonabelian. Thus $|G:A| < |G:A|^2$, again a contradiction to the first assumption.

2A

1. Employ induction on $|G|$. For $|G| = 1$, there is nothing to show. Let H be a subnormal π-subgroup of G. If $H = G$, G itself is a π-subgroup, hence $\mathbf{O}_\pi(G) = G$ and we are done.
So assuming $H < G$, we can find $N < G$ such that $H \lhd\lhd N \trianglelefteq G$. Since $|N| < |G|$, by induction hypothesis $H \subseteq \mathbf{O}_\pi(N)$. Now $\mathbf{O}_\pi(N)$ char $N \trianglelefteq G$, so $\mathbf{O}_\pi(N) \trianglelefteq G$. As $\mathbf{O}_\pi(N)$ is also a π-subgroup of G, we get $H \subseteq \mathbf{O}_\pi(N) \subseteq \mathbf{O}_\pi(G)$.

2. Employ induction on $|G|$. If $|G| = 1$, there is nothing to show. Also if $K = G$, $\mathbf{O}^\pi(G) \subseteq G = K$ and we are done.
So assuming $K < G$, there exists $N < G$ such that $K \lhd\lhd N \trianglelefteq G$. Since $\mathbf{O}^\pi(N)$ is characteristic in N, $\mathbf{O}^\pi(N) \trianglelefteq G$. Since $|G : K| = |G/N||N : K|$ is a π-number, $|G/N|$ and $|N : K|$ are π-numbers. So by induction hypothesis (as $|N| < |G|$) $K \supseteq \mathbf{O}^\pi(N)$. Finally $\left|G / \mathbf{O}^\pi(N)\right| = |G/N| \left|N / \mathbf{O}^\pi(N)\right|$ is a π-number, hence $\mathbf{O}^\pi(N) \supseteq \mathbf{O}^\pi(G)$. Thus $K \supseteq \mathbf{O}^\pi(G)$.

3. a) Employ induction on $|G|$. There is nothing to show for $|G| = 1$. If $H = G$, we are done. Otherwise there exists $N < G$ such that $H \lhd\lhd N \trianglelefteq G$. Now H and $K \cap N$ are subgroups of N and $H \lhd\lhd N$; also $|N : H|$ is relatively prime with $|K \cap N|$. So by induction hypothesis $K \cap N \subseteq H$.
Since $N \trianglelefteq G$, KN is a subgroup and we have

$$|G : H| = |G : KN||KN : N||N : H| = |G : KN||K : K \cap N||N : H|$$

So $|G : H||K \cap N| = |G : KN||K||N : H|$, hence $|G : H||K \cap N|$ is divisible by $|K|$. But $|G : H|$ and $|K|$ are coprime, so $|K \cap N|$ is divisible by $|K|$. This means $K \cap N = K$, so $K \subseteq H$.

b) Employ induction on $|G|$. If $|G| = 1$, OK. If $K = G$, since $|G : H|$ and $|K|$ are coprime, we get $|G : H| = 1$, that is $H = G$. So $K \subseteq H$.
Otherwise there exists $N < G$ such that $K \lhd\lhd N \trianglelefteq G$. HN is a subgroup and we have

$$|G : H| = |G : HN||HN : H| = |G : HN||N : H \cap N|$$

So $H \cap N$ and K are subgroups of N such that $|K|$ and $|N : H \cap N|$ are coprime; with $K \lhd\lhd N$. Hence by induction hypothesis $K \subseteq H \cap N$. Thus $K \subseteq H$.

4. Induct on $|G|$. There is nothing to show for $|G| = 1$. Let $H \lhd\lhd G$. If $H = G$, we are done. Otherwise, there exists $N < G$ such that $H \lhd\lhd N \trianglelefteq G$. $S \cap N \trianglelefteq S$, so there are two cases:

- $S \cap N = S$, that is $S \subseteq N$. Now for every subnormal subgroup K of N, $K \lhd\lhd G$ and hence $KS = SK$ by assumption. By inductive hypothesis we obtain $S \subseteq \mathbf{N}_N(H) \subseteq \mathbf{N}_G(H)$.
- $S \cap N = 1$.

??
??

5. a) Since G is finite, the collection is finite, say $\mathcal{X} = \{M_1, \dots M_r\}$. Start with M_1. If $M_1 = N$, we are done. Otherwise $M_1M_j > M_1$ for some j. WLOG we can assume $j = 2$. Now $M_1 \cap M_2$ is a normal subgroup contained in M_2. Since $M_1M_2 > M_1$, by minimality of M_2 we get $M_1 \cap M_2 = 1$. So M_1M_2 is a direct product.
Now if $N = M_1M_2$ we are done. Otherwise we can assume $M_1M_2M_3 > M_1M_2$. $M_3 \cap M_1M_2$ is a normal subgroup contained in M_3. Since $M_3 \not\subseteq M_1M_2$, minimality of M_3 forces $M_3 \cap M_1M_2 = 1$. Thus $M_1M_2M_3$ is a direct product. If $N = M_1M_2M_3$ we are done. Otherwise we can continue as above. Clearly this process will stop in at most r steps and we will obtain N as a direct product of some subcollection of $\mathcal{X}$.

b) By (a) we can write N as a *direct* product of minimal normal subgroups of G, say $N = M_1M_2 \dots M_k$. We claim that if S is a minimal normal subgroup of M_j for some j, then S is minimal normal in N. Clearly showing $S \trianglelefteq N$ is enough. We have $M_j \subseteq \mathbf{N}_G(S)$. Also since $M_i \cap M_j = 1$ whenever $i \neq j$,

$M_i \subseteq \mathbf{C}_G(M_j) \subseteq \mathbf{C}_G(S)$ for $i \neq j$. Thus N normalizes S.
Therefore for every j we have $\mathrm{Soc}(M_j) \subseteq \mathrm{Soc}(N)$. Now we show that $\mathrm{Soc}(M_j) = M_j$ for every j and it follows that $\mathrm{Soc}(N) = N$. Indeed $1 < \mathrm{Soc}(M_j)$ (as $M_j > 1$) and $\mathrm{Soc}(M_j)$ is characteristic in M_j, hence normal in G; so $\mathrm{Soc}(M_j) = M_j$ since M_j is minimal normal in G.
Finally, let S be a minimal normal subgroup of N. Since $N = \mathrm{Soc}(N)$, reasoning as in (a) we can find minimal normal subgroups $S_2, \dots S_l$ of N such that $N = SS_2 \dots S_l$ where the right hand side is a direct product. Then if $1 < T \trianglelefteq S$, S normalizes T and $S_2, \dots S_l$ centralizes T; hence $T \trianglelefteq N$. By minimality of S we get $T = S$. Thus S is simple.

c) In (b) we established that $\mathrm{Soc}(N) = N$, so N is a product of its minimal normal subgroups, which are all simple by (b). By (a) we can assume this product is direct.

6. Let M be a nonabelian normal subgroup in G and $M \subseteq N$. By 5, we can write $N = M_1 M_2 \dots M_r$ where $M_1, \dots M_r \in \mathcal{X}$ such that the product is direct. For every i, $M \cap M_i$ is a normal subgroup of G contained in M_i. If $M \cap M_i = M_i$ for some i we have $M_i \subseteq M$ and we are done. Otherwise $M \cap M_i = 1$ for all $i = 1, \dots r$. Then $M_i \subseteq \mathbf{C}_G(M)$ for all i, hence $N \subseteq \mathbf{C}_G(M)$ or equivalently $M \subseteq \mathbf{C}_G(N)$. But $M \subseteq N$, hence $M \subseteq \mathbf{Z}(N)$; a contradiction.

7. I couldn't solve this question.

8. Induct on $|G|$. If $|G| = 1$, OK. $S^G \cap T^G$ is a normal subgroup of G contained in S^G, which is minimal normal by 7. Hence either $S^G \cap T^G = 1$ or $S^G \cap T^G = S^G$. In the former case, S^G and T^G are normal subgroups with trivial intersection, hence S^G and T^G commute elementwise. In particular S and T commute elementwise and we are done. In the latter case, we have $1 < S^G \subseteq T^G$. But T^G is also minimal normal in G, hence $S^G = T^G$.
If $S^G < G$, S and T are different nonabelian subnormal simple subgroups of S^G, hence by induction hypothesis S and T commute elementwise; done. If not, $S^G = G$; so G is a minimal normal subgroup of itself hence G is simple. But simple groups have only two subnormal subgroups, and since S and T are nonabelian we get $S = T = G$, contradicting $S \neq T$.

9. I couldn't solve this question.

10. Assume $H \lhd\lhd G$. We employ induction on $|G|$. If $|G| = 1$, OK. If $H = G$, we are done. So assuming $H < G$, we can find $N < G$ such that $H \lhd\lhd N \trianglelefteq G$. If H and H^g are strongly conjugate in G, we can assume $g \in \langle H, H^g \rangle$. Now $H^g \subseteq N^g = N$, so $\langle H, H^g \rangle \subseteq N$ and $g \in N$. Thus H and H^g are also strongly conjugate in N. So by induction hypothesis $H = H^g$.
Conversely, assume H is only strongly conjugate to itself. We induct on $|G|$ to show $H \lhd\lhd G$. Basis case $|G| = 1$ is trivial. If L is any proper subgroup of G that contains H, H is still strongly conjugate to only itself in L. Hence by induction hypothesis $H \lhd\lhd L$ whenever $H \subseteq L < G$.
Suppose H is not subnormal in G. Then the zipper lemma applies, so there is a unique maximal subgroup M containing H. Now for every g, $H \neq H^g$ implies $g \notin \langle H, H^g \rangle$ by assumption. So $\langle H, H^g \rangle$ is a proper subgroup of G that contains H; thus $\langle H, H^g \rangle \subseteq M$. It follows that $H^G \subseteq M$, so $H^G < G$ and hence $H \lhd\lhd H^G \trianglelefteq G$; a contradiction.

2B

1. We just need to blend the proof of Theorem 2.12 and the proof of Theorem 2.8 into one statement. Induct on $|G|$. The basis case $|G| = 1$ is trivial. For every proper subgroup K containing H; for each $k \in K$ either $\langle H, H^k \rangle$ is nilpotent or $HH^k = H^k H$. So by induction hypothesis $H \lhd\lhd K$. Suppose H is not subnormal in G. Then by the zipper lemma there is a unique maximal subgroup M that contains H. Let $g \in G$. There are two cases:

- $\langle H, H^g \rangle$ is nilpotent. Since every subgroup of a nilpotent group is subnormal, $\langle H, H^g \rangle$ is proper in G. Therefore $\langle H, H^g \rangle \subseteq M$.

- $HH^g = H^gH$. Then HH^g is a subgroup in G. Moreover since $H < G$, $HH^g < G$. Thus $HH^g \subseteq M$.

In any case $H^g \subseteq M$. Thus $H^G \subseteq M$, so $H^G < G$. Hence $H \lhd\lhd H^G \trianglelefteq G$, a contradiction.

2. a) By definition, D has a nontrivial cyclic subgroup C such that every element in $D - C$ is an involution. Since $|C| = n$ and n is odd, C does not contain any involution. Hence D contains exactly $|D - C| = n$ involutions.
Let $s \in D - C$. For $c \in C$, by Lemma 2.14a, $c^s = c^{-1}$. So c centralizes s if and only if $c = c^{-1}$. Since C is cyclic of odd order, this means $c = 1$. Let $t \in D - C$ such that $t \neq s$. Then st is a nonidentity element in C. So $ts \neq (ts)^{-1} = st$, i.e t does not centralize s. Therefore $\mathbf{C}_D(s) = \{1, s\}$.
Thus the conjugacy class $[s]$ of s has $|D : \mathbf{C}_D(s)| = n$ elements. Since every element in $[s]$ is an involution, we get $[s] = D - C$.

b) Let C be as above. Now since $|C| = n$ is even and C is cyclic, C contains exactly one involution. Hence D contains exactly $|D - C| + 1 = n + 1$ involutions. Let a be the unique involution in C. For every $s \in D - C$ we have $a^s = a^{-1} = a$ so a commutes with every element in $D - C$. a already commutes with every element in C, so $a \in \mathbf{Z}(D)$.
Fix $s \in D - C$. If $c \in C$ commutes with s, arguing as above we see that c is 1 or a. Let $t \in D - C$ such that $t \neq s$. Then ts is a nonidentity element in C and $ts = st$ means ts is an involution in C, hence $ts = a$; so $t = as$. Therefore $\mathbf{C}_D(s) = \{1, a, s, as\}$.
Thus the conjugacy class $[s]$ has $|D : \mathbf{C}_D(s)| = n/2$ elements. Taking $s' \in (D - C) - [s]$, similarly $[s']$ has $n/2$ elements. Since $a \neq s$ and $[a] = \{a\}$, a and s are not conjugate. Similarly a and s' are not conjugate. So the set $[a] \cup [s] \cup [s']$ has $n + 1$ elements (hence $n + 1$ involutions). Thus the set of involutions of D is precisely $[a] \cup [s] \cup [s']$.

3. Let $D = \langle s, t\rangle$. By Lemma 2.14, D is dihedral; for $C = \langle st\rangle$ we have $|D : C| = 2$; $s, t \in D - C$. Since s and t are not conjugate, by previous exercise C contains an involution z which commutes with both s and t.

4. Suppose G has more than one conjugacy class of involutions. So there exist involutions $s, t \in G$ such that s and t are not conjugate. Then by previous exercise there is an involution $z \in G$, different from s and t such that z commutes with both s and t.
There exist Sylow 2-subgroups P_1, P_2, P_3 such that $s \in P_1$, $t \in P_2$, $z \in P_3$. Since $\langle s, z\rangle$ is a 2-subgroup, it is contained in a Sylow 2-subgroup P_4. Now $s \in P_1 \cap P_4$, hence by assumption (every two distinct Sylow 2-subgroups intersect trivially) we get $P_1 = P_4$. Also $z \in P_3 \cap P_4$, so $P_3 = P_4$. Hence $P_1 = P_3$. $\langle t, z\rangle$ is a 2-subgroup, hence it is contained in a Sylow 2-subgroup P_5. So $t \in P_2 \cap P_5$, hence $P_2 = P_5$. Also $z \in P_1 \cap P_5$, hence $P_1 = P_5$. Thus $P_1 = P_2$.
So s, t lie in the same Sylow 2-subgroup, say P for short.
The above argument shows in general that two non-conjugate involutions lie in the same Sylow 2-subgroup. By assumption there exists $Q \in \mathrm{Syl}_2(G) - \{P\}$. Let u be an involution in Q. Since u and s lie in different Sylow 2-subgroups, we conclude that u and s are conjugate. Similarly u and t are conjugate. Hence s and t are conjugate, a contradiction.

5. (1) $\Rightarrow$ (2): Let $s \in G - B$. Since $|G : B| = 2$, $st \in B$. Then

$$ts = tstt = (st)^t = (st)^{-1} = ts^{-1}$$

Hence $s = s^{-1}$. s cannot be 1, so it is an involution.
(2) $\Rightarrow$ (3): Let $t \in G - B$ and $b \in B$. t is an involution by assumption, also since $bt \in G - B$, bt is also an involution. Then $1 = (bt)^2 = btbt = bb^t$, so $b^t = b^{-1}$.
(3) $\Rightarrow$ (1): Trivial.

6. Assume G has a normal Sylow p-subgroup P. Then since P is the unique Sylow p-subgroup of G, *every* element in G with p-power order lies in P. In particular if $x, y \in G$ have p-power order, $\langle x, y\rangle \subseteq P$ (regardless of whether x and y are conjugate or not); hence $\langle x, y\rangle$ is a p-group.

Conversely, assume that $\langle x, y\rangle$ has a normal Sylow p-subgroup whenever x, y are conjugate elements with p-power order.
Take any $x \in G$ with p-power order and let $H = \langle x\rangle$. Then for every $g \in G$, $\langle H, H^g\rangle = \langle x, x^g\rangle$ has a normal Sylow p-subgroup by assumption, say S. But then as elements with p-power order, x and x^g belong to S. Thus $\langle H, H^g\rangle$ equals S, hence is nilpotent. By Baer's theorem, $H \subseteq \mathbf{F}(G)$, so $x \in \mathbf{O}_p(G)$. Consequently *every* element of G with p-power order lies in $\mathbf{O}_p(G)$, hence $\mathbf{O}_p(G) \in \mathrm{Syl}_p(G)$, as desired.

2C

1. a) Let G be an N-group. A proper homomorphic image of an N-group is isomorphic to G/N for some $1 < N \trianglelefteq G$. Since $1 < N$, there exists a prime p dividing $|N|$. Let $P \in \mathrm{Syl}_p(N)$, then $\mathbf{N}_G(P)$ is solvable by assumption. By the Frattini argument, $G = \mathbf{N}_G(P)N$. Hence

$$G/N = \mathbf{N}_G(P)N \,/N \cong \mathbf{N}_G(P) \,/N \cap \mathbf{N}_G(P)$$

is solvable.

b) Let S be a minimal normal subgroup of G. Suppose there is another minimal normal subgroup T. Then by minimality $S \cap T = 1$. TS is a subgroup of G and $TS > S$. So $T \cong TS/S \subseteq G/S$ is solvable by (a). Since G/T is also solvable, G is solvable; a contradiction. So S is the unique minimal normal subgroup of G.
Clearly S is nonsolvable because G/S is solvable and G is nonsolvable. In particular S is nonabelian. Note that if P is a nonidentity p-subgroup in S, since $\mathbf{N}_S(P) \subseteq \mathbf{N}_G(P)$ and $\mathbf{N}_G(P)$ is solvable by assumption, $\mathbf{N}_S(P)$ is solvable.
Thus S is also a nonsolvable N-group. So S also has a unique minimal normal subgroup, say S'. Then S' is characteristic in S, hence $S' \trianglelefteq G$; therefore minimality of S forces $S = S'$. S is simple.

2D

1. Not

2. yet.