Ch6 Flashcards

Harley Caham Combest

Fa2025 2025-10-24 MATH5353

Chapter 6 — Further Topics in Group Theory

This chapter develops three threads: (1) structure and characterizations of p-groups, nilpotent groups, and solvable groups; (2) applications of Sylow theory and permutation methods to groups of "medium" order (including the unique simple group of order 168); and (3) free groups and presentations, culminating in the universal property of $F(S)$ and practical presentation calculus.

- **p-groups $\Rightarrow$ nilpotent scaffolding.** Key properties of finite p-groups (nontrivial centers; behavior of maximal subgroups; normalizers grow) feed into characterizations of nilpotence and direct-product decompositions by Sylow factors.
- **Techniques for group orders.** Counting elements of prime power order, exploiting small-index subgroups via actions on cosets, comparing Sylow normalizers across primes, and analyzing intersections of Sylow subgroups together rule out simplicity for many n and classify special cases (notably $|G| = 168$).
- **Free groups and presentations.** Construction of $F(S)$, its universal property, and examples/presentations for familiar groups; consequences like Schreier's theorem are noted.

6.1 p-Groups, Nilpotent Groups, and Solvable Groups

Core p-group facts. If $|P| = p^a$ $(a \geq 1)$, then $Z(P) \neq 1$; every nontrivial normal $H \lhd P$ meets $Z(P)$; every maximal subgroup has index p and is normal; and each proper $H < P$ is properly contained in $N_P(H)$. These stem from the class equation and drive induction on $|P|$.

Upper central series and nilpotence. Define $Z_0(G) = 1$ and $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$. A group is *nilpotent* iff $Z_c(G) = G$ for some c (the nilpotence class). Every p-group is nilpotent of class $\leq a - 1$ when $|P| = p^a$.

Equivalent conditions for finite nilpotence. For finite G with Sylow subgroups $P_1, \ldots, P_s$, the following are equivalent:

1. G is nilpotent;
2. every proper $H < G$ is properly contained in $N_G(H)$;
3. all Sylow subgroups are normal;
4. $G \cong P_1 \times \cdots \times P_s$.

As a corollary, finite abelian groups split as direct products of their Sylow subgroups.

Frattini's Argument and maximal subgroups. If $H \lhd G$ and $P \in \mathrm{Syl}_p(H)$, then $G = HN_G(P)$ and $|G : H| \mid |N_G(P)|$. A finite G is nilpotent iff *every* maximal subgroup is normal.

Lower central series and derived series. With $G_1 = [G, G]$ and $G_{i+1} = [G, G_i]$, G is nilpotent $\iff$ $G^n = 1$ for some n (and $Z_i(G) \subseteq G^{\,c-i} \subseteq Z_{i+1}(G)$ when class c). For solvability, the derived series $G^{(0)} = G$, $G^{(i+1)} = [G^{(i)}, G^{(i)}]$ satisfies: G is solvable $\iff$ $G^{(n)} = 1$ for some n. Subgroups and quotients of solvable groups are solvable; extensions with solvable kernel and quotient are solvable.

Selected theorems. Burnside ($|G| = p^a q^b \Rightarrow G$ solvable), Hall's theorem on Sylow complements, Feit–Thompson (odd order $\Rightarrow$ solvable), and Thompson's criterion.

Why this matters. These tools let us detect direct decompositions, prove normality of Sylow subgroups, and bound structure via series, setting up the order-by-order arguments in §6.2.

6.2 Applications in Groups of Medium Order

Playbook of techniques.

1. *Counting elements* of prime/prime-power order across Sylow conjugacy classes to force contradictions or normal Sylow factors.
2. *Small-index subgroups:* actions on G/H give embeddings $G \hookrightarrow S_k$; minimal possible indices constrain n_p and normalizers.
3. *Permutation representations:* compare $N_G(P)$ with $N_{S_k}(P)$ (and with A_k when no index-2 subgroup exists).
4. *Cross-prime leverage:* if P normalizes Q (or vice versa) and $(|P|, |Q|) = 1$, abelianity of PQ can force divisibility constraints on normalizers.
5. *Intersections of Sylow subgroups:* analyze $N_G(P \cap R)$ when $P \neq R$; if $n_p \not\equiv 1 \pmod{p^2}$, there exist $P \neq R$ with $|P \cap R| = |P|/p$.

These methods rule out many candidate simple orders and locate normal subgroups.

Case study: $|G| = 168$. Assuming simplicity, one deduces $n_7 = 8$, $n_3 = 28$, $n_2 = 21$; Sylow-2's are dihedral D_8; $N_G(P_3) \cong S_3$; there are no elements of orders 14 or 21; the conjugacy-class partition has sizes $1, 21, 42, 56, 24, 24$. These data produce a projective-plane incidence geometry (the Fano plane $\mathcal{F}$) on which G acts faithfully, yielding $G \cong \mathrm{Aut}(\mathcal{F}) \cong GL_3(\mathbb{F}_2)$, which is simple and unique of order 168.

Outcomes. Many specific orders (e.g., $380, 396, 2205, \ldots$) are shown non-simple by these tactics; when a simple group exists (order 168) it is rigidly determined.

6.3 A Word on Free Groups

Construction of $F(S)$. Elements are reduced words in $S \cup S^{-1}$; multiplication is concatenation with cancellation. This yields a group with identity the empty word and inverses by reversal/inversion. Associativity can be verified via permutations generated by left-concatenations.

Universal property. For any set map $\psi : S \to G$ into a group G, there exists a unique homomorphism $\varphi : F(S) \to G$ extending ψ. The pair $(F(S), \iota)$ is unique up to unique isomorphism fixing S. Consequences include that every group is a homomorphic image of some free group and that $F(S)$ has no nontrivial relations among the chosen generators.

Presentations. A presentation (S, R) for G records generators and relations so that $G \cong F(S)/\langle\langle R \rangle\rangle$. Examples: $D_{2n} = \langle r, s \mid r^n = s^2 = 1,\ s^{-1}rs = r^{-1} \rangle$, $Q_8 = \langle i, j \mid i^4 = 1,\, i^2 = j^2,\, j^{-1}ij = i^{-1} \rangle$, and finite abelian groups via commuting and power relations. Schreier's theorem: subgroups of free groups are free.

Why this matters. Free groups and presentations supply a language to build and recognize groups, transport maps from generators, and compute (auto)morphisms from relations—tools repeatedly used in earlier chapters and in §6.2's constructions.

6.1: Exercise 3. If G is finite, prove that G is nilpotent if and only if it has a normal subgroup of each order dividing $|G|$, and that G is cyclic if and only if it has a unique subgroup of each order dividing $|G|$.

As General Proposition: For a finite group G, the following hold:
(i) G is nilpotent $\iff$ for every $m \mid |G|$ there exists a normal subgroup $N \lhd G$ with $|N| = m$.
(ii) G is cyclic $\iff$ for every $m \mid |G|$ there is a unique subgroup of order m.

As Conditional Proposition: If $|G| = \prod_{i=1}^{s} p_i^{\alpha_i}$, then G is nilpotent $\iff$ for each $m = \prod_{i=1}^{s} p_i^{\beta_i}$ with $0 \leq \beta_i \leq \alpha_i$ there exists $N \lhd G$ with $|N| = m$. Moreover, G is cyclic $\iff$ for each such m the subgroup of order m is unique.

. . . .

Intuition. Finite nilpotent groups factor as a direct product of their Sylow subgroups. Inside a p-group one can build normal subgroups of every order p^k by climbing through the center one step (p) at a time. Taking products across distinct primes (which commute) produces a *normal* subgroup of any prescribed divisor order. Conversely, if the full prime-power layers are already normal, all Sylow subgroups are normal, hence G is nilpotent. Uniqueness of a subgroup for *every* divisor forces each Sylow to be cyclic and unique, and then the product of generators has order $|G|$.

. . . .

Proof.

Part A (Nilpotent $\Rightarrow$ normal subgroup of every divisor).

Step A1 (Structure). If G is finite nilpotent, then $G \cong P_1 \times \cdots \times P_s$ where each $P_i \in \mathrm{Syl}_{p_i}(G)$ is normal and the P_i pairwise commute.

Step A2 (Key lemma on p-groups). *Claim:* If P is a finite p-group of order p^α, then for each $0 \le k \le \alpha$ there exists a *normal* subgroup $N_k \lhd P$ with $|N_k| = p^k$.

Proof of claim (by induction on k): For $k = 0, 1$ this follows since $1 \lhd P$ and $Z(P) \neq 1$ yields a central (hence normal) subgroup of order p. Suppose $1 < k \le \alpha$. Choose $C \le Z(P)$ with $|C| = p$. By induction applied to P/C, there is a normal subgroup $\overline{N}_{k-1} \lhd P/C$ of order p^{k-1}. Its preimage N_k in P is normal (preimage of a normal subgroup under the quotient map) and has order $p \cdot p^{k-1} = p^k$. This proves the claim.

Step A3 (Assembling the divisor m). Fix $m = \prod_i p_i^{\beta_i} \mid |G|$. For each i pick $H_i \lhd P_i$ with $|H_i| = p_i^{\beta_i}$ from Step A2. Set $N := H_1 \cdots H_s \le P_1 \cdots P_s = G$.

Step A4 (Normality and order). Because distinct Sylow factors commute, conjugation by any $g = (g_1, \dots, g_s) \in G$ acts on H_i as conjugation by $g_i \in P_i$, hence $gH_ig^{-1} = H_i$ (each $H_i \lhd P_i$). Thus $N \lhd G$. Moreover $|N| = \prod_i |H_i| = m$ since the factors have coprime orders and intersect trivially.

Step A5 (Conclusion of A). Therefore G has a normal subgroup of every order $m \mid |G|$.

Part B (Normal subgroup of every divisor $\Rightarrow$ nilpotent).

Step B1 (Normal Sylows). Apply the hypothesis to $m = p_i^{\alpha_i}$: there exists $P_i \lhd G$ with $|P_i| = p_i^{\alpha_i}$, hence $P_i \in \mathrm{Syl}_{p_i}(G)$ is normal for each i.

Step B2 (Direct product). With all Sylow subgroups normal and of pairwise coprime orders, $G = P_1 \cdots P_s \cong P_1 \times \cdots \times P_s$, so G is nilpotent.

Part C (Cyclic $\Rightarrow$ unique subgroup of each divisor).

Step C1 (Standard property). If $G = \langle g \rangle$ has order n, then for each $m \mid n$ the subgroup $\langle g^{n/m} \rangle$ is the unique subgroup of order m.

Part D (Unique subgroup of each divisor $\Rightarrow$ cyclic).
Step D1 (Unique p-subgroups). For each prime $p \mid |G|$, uniqueness gives a single subgroup of order p, hence it is normal; in a p-group, having a unique subgroup of order p forces the Sylow p-subgroup P to be cyclic (otherwise a noncyclic p-group has at least $p+1$ such subgroups).
Step D2 (Unique Sylows). By uniqueness at the top power $p_i^{\alpha_i}$, each Sylow P_i is unique and therefore normal; by D1 each $P_i \cong C_{p_i^{\alpha_i}}$.
Step D3 (Coprime product is cyclic). Let x_i generate P_i. Then $x := x_1 x_2 \cdots x_s$ has order $\operatorname{lcm}(|x_1|, \ldots, |x_s|) = \prod_i p_i^{\alpha_i} = |G|$ (orders are pairwise coprime), so $\langle x \rangle = G$. Hence G is cyclic.

Conclusion. Parts A–B establish the nilpotent equivalence; Parts C–D establish the cyclic equivalence. $\square$

6.1: Exercise 7. Prove that subgroups and quotient groups of nilpotent groups are nilpotent (your proof should work for infinite groups). Give an explicit example of a group G which possesses a normal subgroup H such that both H and G/H are nilpotent but G is not nilpotent.

As General Proposition: If G is a (possibly infinite) nilpotent group of class c, then every subgroup $H \leq G$ and every quotient G/N ($N \lhd G$) is nilpotent of class at most c. Moreover, there exist groups G with a normal subgroup H such that H and G/H are nilpotent but G is not.

As Conditional Proposition: Let G be nilpotent with upper central series $1 = Z_0(G) \leq Z_1(G) \leq \cdots \leq Z_c(G) = G$. Then for any $H \leq G$ we have

$$Z_i(H) \supseteq H \cap Z_i(G) \quad (0 \leq i \leq c),$$

so $Z_c(H) = H$ and hence H is nilpotent of class $\leq c$. For any $N \lhd G$ we have

$$\frac{Z_i(G)N}{N} \leq Z_i(G/N) \quad (0 \leq i \leq c),$$

so $Z_c(G/N) = G/N$ and hence G/N is nilpotent of class $\leq c$. As an explicit counterexample to inheritance in extensions, take $G = S_3$ and $H = A_3 \lhd G$. Then $H \simeq C_3$ and $G/H \simeq C_2$ are nilpotent, but G is not.

. . . .

Intuition. Nilpotence is measured by the upper central series: repeatedly mod out by the center until the group becomes trivial. Subgroups can only gain central elements (intersect the central layers of G), so they reach the top no later than G does. Quotients cannot "lose" centrality coming from G—central layers map to central layers—so they also reach the top no later than G does. The example $S_3 \trianglerighteq A_3$ shows that having a nilpotent normal subgroup and nilpotent quotient does not force the whole group to be nilpotent.

. . . .

Proof.

Step 1 (Upper central series). For any group G, define $Z_0(G) = 1$ and recursively

$$Z_{i+1}(G)/Z_i(G) = Z\big(G/Z_i(G)\big) \qquad (i \geq 0).$$

If $Z_c(G) = G$ for some finite c, then G is nilpotent (of class $\leq c$).

Step 2 (Subgroups inherit central layers). *Claim:* For $H \leq G$ and each $i \geq 0$,

$$H \cap Z_i(G) \;\leq\; Z_i(H).$$

Proof of the claim by induction on i. For $i = 0$ this is $H \cap 1 = 1 = Z_0(H)$. Suppose $H \cap Z_i(G) \leq Z_i(H)$. Consider the inclusions

$$\frac{H \cap Z_{i+1}(G)}{H \cap Z_i(G)} \;\leq\; \frac{Z_{i+1}(G)}{Z_i(G)} = Z\left(\frac{G}{Z_i(G)}\right).$$

Via the natural embedding $H/(H \cap Z_i(G)) \hookrightarrow G/Z_i(G)$ (second isomorphism theorem), the subgroup on the left maps into the center of $H/(H \cap Z_i(G))$. Hence

$$\frac{H \cap Z_{i+1}(G)}{H \cap Z_i(G)} \;\leq\; Z\left(\frac{H}{H \cap Z_i(G)}\right) \cong \frac{Z_{i+1}(H)}{Z_i(H)}.$$

Using the induction hypothesis $H \cap Z_i(G) \leq Z_i(H)$, we conclude $H \cap Z_{i+1}(G) \leq Z_{i+1}(H)$, as claimed.

Step 3 (Subgroups are nilpotent). If $Z_c(G) = G$, then by Step 2,

$$H \;\leq\; H \cap Z_c(G) \;\leq\; Z_c(H) \;\leq\; H,$$

so $Z_c(H) = H$ and H is nilpotent of class $\leq c$. No finiteness was used.

Step 4 (Quotients inherit central layers up to inclusion). Let $\pi : G \to G/N$ be the quotient map with $N \lhd G$. We prove by induction on i that

$$\pi\bigl(Z_i(G)\bigr) \;\le\; Z_i(G/N),$$

equivalently $(Z_i(G)N)/N \le Z_i(G/N)$. For $i = 0$ this is $1 \le 1$. Assume $\pi(Z_i(G)) \le Z_i(G/N)$. Passing to quotients by these terms, we get a surjection

$$\overline{\pi} : \; \frac{G}{Z_i(G)} \longrightarrow \frac{G/N}{\pi(Z_i(G))} \;\le\; \frac{G/N}{Z_i(G/N)}.$$

Since $Z_{i+1}(G)/Z_i(G) = Z\bigl(G/Z_i(G)\bigr)$ is central in $G/Z_i(G)$, its image under $\overline{\pi}$ lies in the center of $(G/N)/Z_i(G/N)$. Translating back, this says

$$\frac{Z_{i+1}(G)N}{N} \;\le\; Z_{i+1}(G/N),$$

completing the induction.

Step 5 (Quotients are nilpotent). If $Z_c(G) = G$, then $(Z_c(G)N)/N = G/N$, and by Step 4 we obtain

$$G/N \;=\; \frac{Z_c(G)N}{N} \;\le\; Z_c(G/N) \;\le\; G/N,$$

so $Z_c(G/N) = G/N$ and G/N is nilpotent of class $\le c$. Again, no finiteness is needed.

Step 6 (Explicit counterexample for extensions). Take $G = S_3$ and $H = A_3 = \langle(1\,2\,3)\rangle \lhd G$. Then $H \simeq C_3$ and $G/H \simeq C_2$ are abelian (hence nilpotent), but G is not nilpotent (in a finite nilpotent group all Sylow subgroups are normal; in S_3 the Sylow-2 subgroups are not).

Conclusion. Subgroups and quotients of nilpotent groups are nilpotent (with class bounded by that of the ambient group), but nilpotence is not, in general, preserved under extensions.

6.1: Exercise 9. Prove that a finite group G is nilpotent if and only if whenever $a, b \in G$ with $(|a|, |b|) = 1$, then $ab = ba$. [*Use Part 4 of Theorem 3.*]

As General Proposition: For a finite group G, the following are equivalent:
(i) G is nilpotent; (ii) whenever $a, b \in G$ have coprime orders, then $ab = ba$.

As Conditional Proposition: If $|G| = \prod_{i=1}^{s} p_i^{\alpha_i}$, then G is nilpotent $\iff$ for every $a, b \in G$ with $(|a|, |b|) = 1$ one has $ab = ba$.

. . . .

Intuition. In a finite nilpotent group the Sylow subgroups are normal and $G \cong P_1 \times \cdots \times P_s$. An element is the product of its components in the distinct Sylow factors; components from different primes commute, so elements of coprime order commute. Conversely, if all coprime-order elements commute, then any two subgroups H, K of coprime orders centralize each other elementwise, so $HK = KH$ is a subgroup (indeed $H \times K$). By Part 4 of Theorem 3 ("finite nilpotence $\iff$ Sylow factors permute / G is the direct product of its Sylow subgroups"), this forces G to be nilpotent.

. . . .

Proof.

Step 1 (Nilpotent $\Rightarrow$ coprime orders commute). If G is nilpotent, then each Sylow $P_i \lhd G$ and $G \cong P_1 \times \cdots \times P_s$. Write $a = a_1 \cdots a_s$ and $b = b_1 \cdots b_s$ with $a_i, b_i \in P_i$. If $(|a|, |b|) = 1$, then for each i at least one of a_i, b_i is 1 (orders in a p_i-group are powers of p_i). Hence a_i and b_j lie in different Sylow factors for $i \neq j$ and therefore commute; thus $ab = ba$.

Step 2 (Coprime-order commutation $\Rightarrow$ coprime-order subgroups permute). Let $H, K \leq G$ with $(|H|, |K|) = 1$. For $h \in H$ and $k \in K$, $|h| \mid |H|$ and $|k| \mid |K|$, so $(|h|, |k|) = 1$ and by hypothesis $hk = kh$. Hence every h commutes with every k, so $HK = KH$ and HK is a subgroup (indeed isomorphic to $H \times K$).

Step 3 (Apply Theorem 3, Part 4). Part 4 of Theorem 3 asserts that a finite group is nilpotent iff its Sylow subgroups are normal (equivalently, iff subgroups of coprime orders permute and G is the internal direct product of its Sylow subgroups). By Step 2, subgroups of coprime orders permute; in particular the Sylow subgroups permute and are normal. Therefore G is the (internal) direct product of its Sylow subgroups and hence nilpotent.

Conclusion. Steps 1–3 establish the stated equivalence. □

. . . .

Alternative check (within a single cyclic subgroup). For any $g \in G$ with $|g| = p^\alpha r$ and $(p, r) = 1$, the elements g^r (a p-element) and g^{p^α} (a p'-element) commute and multiply to g. If coprime-order elements centralize every p-subgroup, then conjugation by any g on a Sylow p-subgroup reduces to conjugation by g^r, a p-element, sending Sylow p-subgroups to Sylow p-subgroups; combined with Step 2 this again yields normal Sylows and nilpotence.

6.1: Exercise 10. Prove that D_{2n} is nilpotent if and only if n is a power of 2. [*Use Exercise 9.*]

As General Proposition: For the dihedral group $D_{2n} = \langle r, s \mid r^n = 1,\ s^2 = 1,\ srs = r^{-1} \rangle$ of order $2n$, we have

$$D_{2n} \text{ is nilpotent} \iff n = 2^k \text{ for some } k \geq 0.$$

As Conditional Proposition: If $n = 2^k$, then $|D_{2n}| = 2^{k+1}$ is a 2-power, hence D_{2n} is nilpotent; if n has an odd prime factor p, then there exist $a, b \in D_{2n}$ with $(|a|, |b|) = 1$ but $ab \neq ba$, so by Exercise 9 the group is not nilpotent.

. . . .

Intuition. Nilpotence for finite groups is equivalent to "elements of coprime order commute" (Exercise 9). In D_{2n}, the rotation r has order n and a reflection s has order 2. If n contains an odd prime p, then $a = r^{n/p}$ has order p and $b = s$ has order 2, yet $sas^{-1} = r^{-n/p} \neq r^{n/p}$, so a and b do not commute—hence D_{2n} is not nilpotent. When n is a power of 2, D_{2n} is a finite 2-group, and every finite p-group is nilpotent.

. . . .

Proof.

Step 1 (Presentation and basic orders). Write $D_{2n} = \langle r, s \mid r^n = 1,\ s^2 = 1,\ srs = r^{-1}\rangle$. Then $|r| = n$ and $|s| = 2$.

Step 2 (n a power of 2 $\Rightarrow$ nilpotent). If $n = 2^k$, then $|D_{2n}| = 2^{k+1}$ is a power of 2; hence D_{2n} is a finite 2-group and therefore nilpotent.

Step 3 (n not a power of 2 produces coprime noncommuters). Suppose n has an odd prime divisor p. Let $a = r^{n/p}$; then $|a| = p$. Let $b = s$; then $|b| = 2$ and $(|a|, |b|) = 1$. Compute

$$bab^{-1} = sas = r^{-n/p} \neq r^{n/p} = a$$

because $a = r^{n/p} = r^{-n/p}$ would force $r^{2n/p} = 1$, i.e. $n \mid 2n/p$, which is equivalent to $p \mid 2$, impossible since p is odd. Thus $ab \neq ba$.

Step 4 (Invoke Exercise 9). By Exercise 9, a finite group is nilpotent iff any two elements of coprime orders commute. Step 3 provides elements of coprime orders that do *not* commute when n has an odd prime factor, so D_{2n} is not nilpotent in that case.

Step 5 (Conclusion). Combining Steps 2 and 4: D_{2n} is nilpotent exactly when n is a power of 2. $\square$

Additional Exercise 1. Let N and H be groups. Let $\varphi : H \to \mathrm{Aut}(N)$ be a homomorphism and identify N and H as subgroups of the semidirect product $G = N \rtimes_\varphi H$.
(i) Prove that $C_H(N) = \ker \varphi$.
(ii) Prove that $C_N(H) = N_N(H)$.

As General Proposition: In $G = N \rtimes_\varphi H$ with the standard embeddings $N \simeq N \times \{1\}$ and $H \simeq \{1\} \times H$, we have $C_H(N) = \ker \varphi$ and $C_N(H) = N_N(H)$.

As Conditional Proposition: Write elements as pairs with multiplication $(n_1, h_1)(n_2, h_2) = (n_1\, \varphi(h_1)(n_2),\, h_1 h_2)$, $n_i \in N$, $h_i \in H$. Then

$$h \in H \text{ centralizes } N \iff \varphi(h) = \mathrm{id}_N, \qquad n \in N \text{ normalizes } H \iff \varphi(h)(n) = n\, \forall h \in H,$$

whence $C_H(N) = \ker \varphi$ and $C_N(H) = N_N(H)$.

. . . .

Intuition. In a semidirect product, H acts on N by the given φ. Conjugating an element of N by an element of H applies exactly this automorphism; thus h commutes with every n iff h acts trivially on N, i.e. $h \in \ker\varphi$. Likewise, conjugating an element of H by an element $n \in N$ stays inside H precisely when n is fixed by every h under the action—equivalently, when n commutes with H in G.

. . . .

Proof.

Step 1 (Model and embeddings). View G as the set $N \times H$ with $(n_1, h_1)(n_2, h_2) = (n_1\,\varphi(h_1)(n_2),\ h_1h_2)$ and inverses $(n, h)^{-1} = (\varphi(h^{-1})(n^{-1}), h^{-1})$. Identify N with $\{(n, 1)\}$ and H with $\{(1, h)\}$.

Step 2 (Conjugation of N by H). For $h \in H$ and $n \in N$,

$$(1, h)(n, 1)(1, h)^{-1} = (1, h)(n, 1)(1, h^{-1}) = (\varphi(h)(n), 1).$$

Therefore h commutes with all $n \in N$ iff $\varphi(h)(n) = n$ for all n, i.e. $\varphi(h) = \mathrm{id}_N$. Hence $C_H(N) = \ker\varphi$.

Step 3 (Conjugation of H by N). For $n \in N$ and $h \in H$,

$$(n, 1)(1, h)(n, 1)^{-1} = (n, h)(n^{-1}, 1) = (n\,\varphi(h)(n^{-1}),\ h).$$

This element lies in the embedded copy of H (i.e. has first coordinate 1) iff $n\,\varphi(h)(n^{-1}) = 1$, i.e. $\varphi(h)(n) = n$. Thus n normalizes H ($nHn^{-1} = H$) iff $\varphi(h)(n) = n$ for all $h \in H$.

Step 4 (Centralizer of H inside N). By definition in G, $n \in C_N(H)$ iff $(n, 1)$ commutes with every $(1, h)$, equivalently iff $(n, 1)(1, h) = (1, h)(n, 1)$ for all h. Using Step 3, this is exactly the same condition $\varphi(h)(n) = n$ for all $h \in H$. Therefore

$$C_N(H) = \{n \in N :\ \varphi(h)(n) = n\ \forall h \in H\}.$$

Comparing with Step 3, the same condition characterizes $N_N(H) = \{n \in N : nHn^{-1} = H\}$. Hence $C_N(H) = N_N(H)$.

Conclusion. In $G = N \rtimes_\varphi H$, $C_H(N) = \ker\varphi$ and $C_N(H) = N_N(H)$. $\square$

Additional Exercise 2. Let $G = (\mathbb{Z}/2 \times \mathbb{Z}/2) \rtimes \mathrm{Aut}(\mathbb{Z}/2 \times \mathbb{Z}/2)$ (with the natural action).
(i) Prove that $G = N \rtimes H$ where $N = \mathbb{Z}/2 \times \mathbb{Z}/2$ and $H \simeq S_3$. Deduce that $|G| = 24$.
(ii) Prove that $G \simeq S_4$. (Obtain a homomorphism $G \to S_4$ by the action on the left cosets of H; use Problem 1 to show the representation is faithful.)

As General Proposition: Writing $V := \mathbb{Z}/2 \times \mathbb{Z}/2$, one has $\mathrm{Aut}(V) \cong S_3$ and hence

$$G \;=\; V \rtimes \mathrm{Aut}(V) \;\cong\; V \rtimes S_3, \qquad |G| = |V| \cdot |\mathrm{Aut}(V)| = 4 \cdot 6 = 24,$$

and the natural action of G on the four left cosets of the subgroup $H \simeq S_3$ yields an isomorphism $G \cong S_4$.

As Conditional Proposition: Let $N := V \cong C_2 \times C_2$ and let $H := \mathrm{Aut}(V)$. Then $G = N \rtimes H$ with $H \cong S_3$. The coset action

$$\rho : G \longrightarrow S_{[G:H]} = S_4$$

is faithful (its kernel is $\bigcap_{g \in G} gHg^{-1} = \{1\}$), hence $G \cong S_4$.

. . . .

Intuition. The group $V = C_2 \times C_2$ has exactly three nontrivial elements; automorphisms permute these three, so $\mathrm{Aut}(V) \cong S_3$. Thus $G = V \rtimes S_3$ has order $4 \cdot 6 = 24$. An index-4 subgroup $H \cong S_3$ gives a degree-4 permutation representation. Its kernel is the core $\bigcap gHg^{-1}$. In a semidirect product $V \rtimes_\varphi H$, conjugating $(1, h)$ by $(v, 1)$ lands in H iff $\varphi(h)$ fixes v; therefore $\bigcap_{v \in V}(v, 1)H(v, 1)^{-1} = \ker \varphi$. Here $\varphi : H \to \mathrm{Aut}(V)$ is the identity, so $\ker \varphi = 1$, making the action faithful and forcing an isomorphism onto S_4.

. . . .

Proof.

Step 1 (Identify H). The nonzero elements of $V = \mathbb{F}_2^2$ are the three vectors of order 2. Every automorphism permutes these three, and every permutation is realized by some invertible linear map; hence $\mathrm{Aut}(V) \cong S_3$.

Step 2 (Semidirect description). By definition $G = V \rtimes_{\mathrm{id}} \mathrm{Aut}(V)$, so with $N := V$ and $H := \mathrm{Aut}(V)$ we have $G = N \rtimes H$ and $H \cong S_3$.

Step 3 (Order). Since $|V| = 4$ and $|\mathrm{Aut}(V)| = 6$, we have $|G| = 4 \cdot 6 = 24$.

Step 4 (Coset action gives $\rho : G \to S_4$). The subgroup H has index $[G : H] = 4$. Let ρ be the permutation representation of G on the 4 left cosets of H; thus $\rho : G \to S_4$ is a homomorphism.

Step 5 (Compute the core using Problem 1). In the semidirect product model $(v, h) \in V \rtimes H$, Problem 1 gives

$$(n, 1)(1, h)(n, 1)^{-1} = (n\, h(n)^{-1}, h).$$

This lies in the embedded copy of H iff $h(n) = n$. Hence

$$\bigcap_{n \in V}(n, 1)H(n, 1)^{-1} = \{(1, h) : h(n) = n \ \forall n \in V\} = \ker\big(H \xrightarrow{\mathrm{id}} \mathrm{Aut}(V)\big) = 1.$$

Therefore the core $\bigcap_{g \in G} gHg^{-1}$ is trivial, so $\ker \rho = \{1\}$ and ρ is faithful.

Step 6 (Conclude $G \cong S_4$). The image $\rho(G)$ is a transitive subgroup of S_4 of order $|G|/|\ker \rho| = 24$. Since $|S_4| = 24$, we have $\rho(G) = S_4$ and ρ is an isomorphism. Thus $G \cong S_4$. ∎