Math 594. Solutions 4

Book problems §4.5:

6. Exhibit all Sylow 3-subgroups of $\mathfrak{S}_4$ and $\mathfrak{A}_4$.

Solution: Any Sylow 3-subgroup of $\mathfrak{S}_4$ or $\mathfrak{A}_4$ has size 3 and is therefore generated by an element of order 3. Hence, the Sylow 3-subgroups are specified by elements of order 3 that generate the same subgroup. Observe that the Sylow 3-subgroups of $\mathfrak{S}_4$ and $\mathfrak{A}_4$ are the same since $\mathfrak{A}_4$ contains all elements of order 3 in $\mathfrak{S}_4$. Thus, the Sylow 3-subgroups of $\mathfrak{S}_4, \mathfrak{A}_4$ are given as

$$H_1 = \langle(123)\rangle \qquad H_2 = \langle(124)\rangle \qquad H_3 = \langle(134)\rangle \qquad H_4 = \langle(234)\rangle.$$

7. Exhibit all Sylow 2-subgroups of $\mathfrak{S}_4$ and find elements of $\mathfrak{S}_4$ which conjugate one of these into each of the others.

Solution: The Sylow 2-subgroups of $\mathfrak{S}_4$ have size 8 and the number of Sylow 2-subgroups is odd and divides 3. Counting shows that $\mathfrak{S}_4$ has 16 elements of order dividing 8, and since every 2-subgroup is contained in a Sylow 2-subgroup, there cannot be only one Sylow 2-subgroup. More counting reveals that $\mathfrak{S}_4$ contains six 2-cycles, three 2×2-cycles, and six 4-cycles. Since the three Sylow 2-subgroups of $\mathfrak{S}_4$ are conjugate, the different cycle types must be distributed "evenly" among the three Sylow 2-subgroups. Since we have three Sylow 2-subgroups and only 16 elements to fill them with, any two Sylow 2-subgroups must intersect. Moreover, we know exactly how they intersect: recall that the klein 4-group V_4 is normal in $\mathfrak{S}_4$ since it is a union of conjugacy classes. Therefore, each Sylow 2-subgroup contains V_4 (since in particular some Sylow 2-subgroup does and all Sylow 2-subgroups are conjuate). We have determined that each Sylow 2-subgroup contains two (disjoint) 2-cycles, all three 2×2-cycles, and two 4-cycles (each squaring to one of the 2×2-cycles and obviously inverses of eachother). Therefore, the 3 Sylow 2-subgroups of $\mathfrak{S}_4$ are:

$$H_1 = \{1, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423), \}$$
$$H_2 = \{1, (13), (24), (12)(34), (13)(24), (14)(23), (1234), (1432), \}$$
$$H_3 = \{1, (14), (23), (12)(34), (13)(24), (14)(23), (1342), (1243), \}.$$

To determine elements of $\mathfrak{S}_4$ that conjugate H_1 to H_2, H_3, it is enough to find elements that conjugate a 2-cycle in H_1 to a 2-cycle in H_2, H_3. Observe that $(124)(12)(142) = (24)$ and $(123)(12)(132) = (23)$ so that $(124)H_1(142) = H_2$ and $(123)H_1(132) = H_3$.

13. Prove that a group of order 56 has a normal Sylow p-subgroup for some prime p dividing its order.

Solution: Let G be a group with $|G| = 56 = 2^3 \cdot 7$ so that the number of Sylow 2-subgroups of G is 1 or 7 and the number of Sylow 7-subgroups is 1 or 8. Suppose that G does not have a normal Sylow 7-subgroup. Then there are 8 Sylow 7-subgroups. Now the intersection of two distinct Sylow 7-subgroups must be trivial since every nontrivial element of a group of order 7 generates the group. It is clear that the intersection of any Sylow 2-subgroup with any Sylow 7-subgroup is also trivial. Therefore, G contains 48 elements of order 7. This leaves $56 - 48 = 8$ elements not of order 7, so that we have exactly *one* Sylow 2-Subgroup. Hence, G has a normal Sylow p-subgroup for $p = 2$ or 7.

25. Prove that if G is a group of order 385 then $Z(G)$ contains a Sylow 7-subgroup of G and a Sylow 11-subgroup is normal in G.

Solution: Observe that $|G| = 385 = 5 \cdot 7 \cdot 11$. The number of Sylow 11-subgroups of G divides 35 and is congruent to 1 mod 11. The only possibility is that there is a unique (and hence normal) Sylow 11-subgroup of G. Similarly, the number of Sylow 7-subgroups of G divides 55 and is congruent to 1 mod 7. Again, the only possibility is that there is a unique Sylow 7-subgroup of G. Let H be the unique Sylow 7-subgroup of G. Now G acts on H by conjugation so we have a map $G \to \mathrm{Aut}(H) \simeq (\mathbf{Z}/7)^\times$ with kernel $Z_G(H)$. It follows that $G/Z_G(H) \hookrightarrow \mathrm{Aut}(H)$ so that $G/Z_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$. Since H is cyclic, (it is of prime order) we have $H \leqslant Z_G(H)$ so that $|G/Z_G(H)||55$. But $\mathrm{Aut}(H) \simeq (\mathbf{Z}/7)^\times$ has order 6 so that the image of $G/Z_G(H)$ must have size dividing 6 and 55. Hence, $G/Z_G(H) = \{1\}$ so that $H \leqslant Z_G(H) = G$, i.e., the unique Sylow 7-subgroup of G is contained in $Z(G)$.

Book problems §5.5:

6. Assume that K is a cyclic group, H an arbitrary group and $\varphi_i : K \to \mathrm{Aut}(H)$ for $i = 1, 2$ are homomorphisms with $\varphi_1(K)$ conjugate to $\varphi_2(K)$ as subgroups of $\mathrm{Aut}(H)$. If K is infinite, assume that φ_i are injective. Prove by constructing an explicit isomorphism that $H \rtimes_{\varphi_1} K \simeq H \rtimes_{\varphi_2} K$.

Solution: Write $\varphi_1(K) = \sigma\varphi_2(K)\sigma^{-1}$ for some $\sigma \in \mathrm{Aut}(H)$. Assume first that K is finite. Since $\varphi_1(K) \simeq \varphi_2(K)$ (recall that conjugation by any element of a group G is an automorphism of G) we see that $\ker(\varphi_1), \ker(\varphi_2)$ have the same size ($|K|/|\varphi_i(K)|$ for $i = 1, 2$). Now K is cyclic and hence there is a unique subgroup of any given order dividing $|K|$ so that $\ker(\varphi_1) = \ker(\varphi_2) := K'$. It follows that φ_i give isomorphisms $K/K' \simeq \varphi_i(K)$ and hence that $\varphi_2^{-1}c_\sigma\varphi_1 \in \mathrm{Aut}(K/K')$ where $c_\sigma : \mathrm{Aut}(H) \to \mathrm{Aut}(H)$ denotes conjugation by σ. Now $K/K' \simeq \mathbf{Z}/m$ for some $m||K|$ since K is cyclic, so that $\mathrm{Aut}(K/K') \simeq (\mathbf{Z}/m)^\times$ and we identify $\varphi_2^{-1}c_\sigma\varphi_1 \in \mathrm{Aut}(K/K')$ with some $u \in (\mathbf{Z}/m)^\times$. Now if we let $|K| = n$ than $\mathrm{Aut}(K) \simeq (\mathbf{Z}/n)^\times$. Since the natural map $(\mathbf{Z}/n)^\times \to (\mathbf{Z}/m)^\times$ (given by reduction modulo m, since $m|n$) is surjective, there exists a lift $a \in (\mathbf{Z}/n)^\times$ of u so that $\varphi_1(k) = \sigma\varphi_2(k)^a\sigma^{-1}$ for all $k \in K$, with $k \to k^a$ an automorphism of K. Since $k \mapsto k^a$ is an automorphism of K, and $|K|$ is finite, there exists some b such that $k^{ab} = k$.

In the case that K is infinite, let k_0 generate K. Then since $\varphi_1(K) = \sigma\varphi_2(K)\sigma^{-1}$ we have $\varphi_1(k_0) = \sigma\varphi_2(k_0^a)\sigma^{-1}$ for some a from which it follows that $\varphi_1(k) = \sigma\varphi_2(k^a)\sigma^{-1}$ for all $k \in K$. Similarly, there exists some $b \in \mathbf{Z}$ such that $\varphi_2(k) = \sigma^{-1}\varphi_1(k^b)\sigma$ for all $k \in K$, from which it follows that $\varphi_i(k^{ab}) = \varphi_i(k)$ for $i = 1, 2$. Since in this case we assume that φ_i is injective, we must have $k^{ab} = k$ for all k.

Now define $\psi : H \rtimes_{\varphi_1} K \to H \rtimes_{\varphi_2} K$ by $(h, k) \mapsto (\sigma(h), k^a)$. Similarly, define $\phi : H \rtimes_{\varphi_2} K \to H \rtimes_{\varphi_1} K$ by $(h, k) \mapsto (\sigma^{-1}(h), k^b)$. Then it is not hard to verify that

$$\phi \circ \psi(h, k) = (\sigma^{-1}\sigma(h), k^{ba}) = (h, k)$$

and

$$\psi \circ \phi(h, k) = (\sigma\sigma^{-1}(h), k^{ab}) = (h, k).$$

We check that ψ is a group homomorphism; the corresponding check for ϕ is virtually identical. Let us denote by $x \cdot_\varphi y$ the product of $x, y \in H \rtimes_\varphi K$. We have:

$$\begin{aligned}
\psi((h_1, k_1) \cdot_{\varphi_1} (h_2, k_2)) &= \psi(h_1\varphi_1(k_1)(h_2), k_1k_2) \\
&= (\sigma(h_1\varphi_1(k_1)(h_2)), k_1^a k_2^a) \\
&= (\sigma(h_1)\sigma\varphi_1(k_1)\sigma^{-1}\sigma(h_2), k_1^a k_2^a) \\
&= (\sigma(h_1)\varphi_2(k_1^a)\sigma(h_2), k_1^a k_2^a) \\
&= (\sigma(h_1), k_1^a) \cdot_{\varphi_2} (\sigma(h_2), k_2^a) \\
&= \psi(h_1, k_1) \cdot_{\varphi_2} \psi(h_2, k_2),
\end{aligned}$$

where we have used the fact that K is cyclic on the second line. Thus, ψ is a group homomorphism with a two-sided inverse homomorphism, ϕ, so that ψ gives an isomorphism $\psi : H \rtimes_{\varphi_1} K \simeq H \rtimes_{\varphi_2} K$.

7. This exercise describes 13 isomorphism types of groups of order 56.

   (a) Prove that there are 3 abelian groups of order 56.

   Solution: From HW 2, Problem 2, we know that every finite abelian group has a unique decomposition as the product of cyclic groups in invariant factor form. It follows that there are 3 non-isomorphic abelian groups of order 56:

   $$(\mathbf{Z}/2) \times (\mathbf{Z}/2) \times (\mathbf{Z}/14) \qquad (\mathbf{Z}/2) \times (\mathbf{Z}/28) \qquad \mathbf{Z}/56.$$

(b) Prove that every group of order 56 has either a normal Sylow 2-subgroup or a normal Sylow 7-subgroup.

Solution: This was done in §4.5, Problem 13 above.

(c) Construct the following non-abelian groups of order 56 which have a normal Sylow 7-subgroup and whose Sylow 2-subgroup S is as specified:
- one group when $S \simeq \mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/2$.
- two non-isomorphic groups when $S \simeq \mathbf{Z}/4 \times \mathbf{Z}/2$.
- one group when $S \simeq \mathbf{Z}/8$.
- two non-isomorphic groups when $S \simeq Q_8$.
- three non-isomorphic groups when $S \simeq D_8$.

Solution:
- Let $G = \mathbf{Z}/7 \rtimes_\varphi S$ where $S \simeq \mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/2$ and $\varphi : S \to \mathrm{Aut}(\mathbf{Z}/7) \simeq (\mathbf{Z}/7)^\times = \langle \sigma \rangle$ is given by $\varphi(x, y, z) = \sigma^{3(x+y+z)}$, so that

$$(a, (x, y, z))(b, (u, v, w)) = (a + \sigma^{3(x+y+z)}(b), (x + u, y + v, z + w)).$$

Observe that any nontrivial homomorphism $\varphi : S \to (\mathbf{Z}/7)^\times \simeq \mathbf{Z}/6$ must take some element of $s \in S$ to σ^3. Then being a homomorphism, if $\varphi(t) = 1$ we must have $\varphi(s + t) = \sigma^3$. It follows that φ sends exactly half of S to σ^3 and the other half to 1. In other words, any such nontrivial homomorphism φ is completely determined by specifying as its kernel one of the subgroups of S of order 4. Since every non-trivial element of S has order 2, there is no way to tell elements apart, so that, by relabelling the generators of S, we have an isomorphism $\mathbf{Z}/7 \rtimes_{\varphi_1} S \simeq \mathbf{Z}/7 \rtimes_{\varphi_2} S$ for any $\varphi_1, \varphi_2 : S \to \mathrm{Aut}(\mathbf{Z}/7)$.
- Let $G = \mathbf{Z}/7 \rtimes_\varphi S$ where $S = \mathbf{Z}/4 \times \mathbf{Z}/2$. Let $\varphi_i : S \to \mathrm{Aut}(\mathbf{Z}/7) = \langle \sigma \rangle \simeq \mathbf{Z}/6$ for $i = 1, 2$ be given by $\varphi_1(1, 0) = \sigma^3, \varphi_1(0, 1) = 1$ and $\varphi_2(1, 0) = 1, \varphi_2(0, 1) = \sigma^3$. It is not hard to see that up to relabelling the generators of S these are the only two homomorphisms of S into $\mathrm{Aut}(\mathbf{Z}/7)$ and that we get two non-isomorphic groups $\mathbf{Z}/7 \rtimes_{\varphi_1} S$ and $\mathbf{Z}/7 \rtimes_{\varphi_2} S$. Indeed, as above, a nontrivial homomorphism $\varphi : S \to \mathrm{Aut}(\mathbf{Z}/7)$ is determined by specifying it's kernel as a subgroup of order 4 of S (since any nontrivial homomorphism must map S surjectively onto the unique copy of $\mathbf{Z}/2 < \mathbf{Z}/6 \simeq \mathrm{Aut}(\mathbf{Z}/7)$). Up to isomorphism, there are precisely two distinct subgroups of S of order 4: one isomorphic to $\mathbf{Z}/4$ and one isomorphic to $\mathbf{Z}/2 \times \mathbf{Z}/4$. Observe that φ_1 has kernel isomorphic to $\mathbf{Z}/2 \times \mathbf{Z}/2$ while φ_2 has kernel isomorphic to $\mathbf{Z}/4$, so that the semi-direct products $\mathbf{Z}/7 \rtimes_{\varphi_1} S$ and $\mathbf{Z}/7 \rtimes_{\varphi_2} S$ have *different* centers and are hence not isomorphic.
- Let $G = \mathbf{Z}/7 \rtimes_\varphi S$ where $S = \mathbf{Z}/8$ and let $\varphi : S \to \mathrm{Aut}(\mathbf{Z}/7) = \langle \sigma \rangle$ be given by $\varphi(1) = \sigma^3$. Again, any nontrivial homomorphism $\varphi : S \to \mathrm{Aut}(\mathbf{Z}/7)$ must have kernel a subgroup of S of order 4 and is completely determined by this kernel. Since there is a unique subgroup of $\mathbf{Z}/8$ of order 4, there is a unique nontrivial such φ. Another way to see uniqueness of φ is to use Problem 6, and the fact that $\mathbf{Z}/8$ is cyclic and any nontrivial homomorphism $\varphi : S \to \mathrm{Aut}(\mathbf{Z}/7)$ must give an isomorphism $S/\ker(\varphi) \simeq \mathbf{Z}/2 < \mathbf{Z}/6 \simeq \mathrm{Aut}(\mathbf{Z}/7)$, so that the images of any two nontrivial homomorphisms must coincide.
- Let $G = \mathbf{Z}/7 \rtimes_\varphi S$ where $S = Q_8$. Now any nontrivial homomorphism $\varphi : S \to \mathrm{Aut}(\mathbf{Z}/7)$ must map S surjectively onto the unique copy of $\mathbf{Z}/2$ in $\mathrm{Aut}(\mathbf{Z}/7)$, and is completely determined by specifying as its kernel a subgroup of $S = \langle \mathbf{i}, \mathbf{j} \rangle$ of order 4. By HW 2, Problem 1, we have seen that S has three subgroups of order 4 given by $H_1 = \langle \mathbf{i} \rangle,\ H_2 = \langle \mathbf{j} \rangle,\ H_3 = \langle \mathbf{ij} \rangle$. However, these 3 subgroups are clearly isomorphic so that, up to automorphism of S, there is a unique nontrivial homomorphism $\varphi_1 : S \to \mathrm{Aut}(\mathbf{Z}/7) = \langle \sigma \rangle$ given by $\varphi_1(\mathbf{i}) = \varphi_1(\mathbf{j}) = \sigma^3$. However, we also have the trivial homomorphism $\varphi_2 : S \to \mathrm{Aut}(\mathbf{Z}/7)$ determined by mapping all of S to the identity. In this case, S centralizes $\mathbf{Z}/7$, while in the former, the centralizer of $\mathbf{Z}/7$ is a proper subgroup of S so that these two semidirect products are not isomorphic. It is clear that both constructions give nonabelian groups.

- $G = \mathbf{Z}/7 \rtimes_\varphi S$ where $S = D_4$. Again, we determine the homomorphisms $\varphi : S \to \mathrm{Aut}(\mathbf{Z}/7)$ that give rise to non-isomorphic semidirect products G. As above, any homomorphism is completely determined by specifying a subgroup of order 4 or 8 of D_4 as its kernel. The nonisomorphic subgroups of order 4 of D_4 are isomorphic to $\mathbf{Z}/4$ and $\mathbf{Z}/2 \times \mathbf{Z}/2$ (if $D_4 = \langle r, s : r^4 = s^2 = 1,\ rs = sr^{-1}\rangle$ is a presentation then $\langle r\rangle \simeq \mathbf{Z}/4$ and $\langle r^2, s\rangle \simeq \mathbf{Z}/2 \times \mathbf{Z}/2$). This gives three homomorphisms $\varphi_i : S \to \mathrm{Aut}(\mathbf{Z}/7) = \langle\sigma\rangle$ for $i = 1, 2, 3$, with

$$\varphi_1(r) = \sigma^3 \qquad \varphi_2(r) = 1 \qquad \varphi_3(r) = 1$$
$$\varphi_1(s) = 1 \qquad \varphi_2(s) = \sigma^3 \qquad \varphi_3(s) = 1.$$

  Moreover, we see that the semidirect products $G_i = \mathbf{Z}/7 \rtimes_{\varphi_i} S$ for $i = 1, 2, 3$ are nonisomorphic since the centralizers in S of $\mathbf{Z}/7$ are isomorphic to $\mathbf{Z}/2 \times \mathbf{Z}/2,\ \mathbf{Z}/4,\ S$ for $i = 1, 2, 3$ respectively.

(d) Let G be a group of order 56 with a non-normal Sylow 7-subgroup. Prove that if S is the Sylow 2-subgroup of G then $S \simeq \mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/2$.

Solution: Let H be any Sylow 7-subgroup of G. Then clearly $H \cap S = \{1\}$ by order considerations. Now H acts on S by conjugation, and $Z_H(S)$ is a subgroup of H. Since $|H| = 7$, it follows that $Z_H(S) = \{1\}$ or H. But if $Z_H(S) = H$ then $hs = sh$ for all $s \in S$ and $h \in H$; so that $sHs^{-1} = H$ and HS is a subgroup of G of order 56, i.e. $HS = G$. Since H clearly normalizes H (it even centralizes H, since H is abelian), it follows that G normalizes H, and this is a contradiction. Hence $Z_H(S) = \{1\}$ so that H acts transitively (by conjugation) on the 7 nonidentity elements of S. Since conjugation preserves order, it follows that all 7 nonidentity elements of S have the same order. Clearly this order must be 2 (otherwise there would be elements of different order, since for example, any order 4 element has square of order 2). But if $g \in S$ has order 2 then $g = g^{-1}$; so that for $a, b \in S$ we have $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$ whence S is abelian. The only abelian group of order 8 with all nontrivial elements having order 2 is (up to isomorphism) $\mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/2$.

(e) Prove that there is a unique group of order 56 with a non-normal Sylow 7-subgroup.

Solution: By part (d) we know that any such group must be isomorphic to $\mathbf{Z}/7 \ltimes_\varphi (\mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/2)$ for some nontrivial $\varphi : \mathbf{Z}/7 \to \mathrm{Aut}(\mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/2) \simeq \mathrm{GL}_3(\mathbf{F}_2)$. It is not difficult to compute that $|\mathrm{GL}_3(\mathbf{F}_2)| = 168 = 2^3 \cdot 3 \cdot 7$ so that by the Sylow Theorems, $\mathrm{Aut}(\mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/2)$ contains an element of order 7. (Indeed, by inspection one finds that

$$s := \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \in \mathrm{GL}_3(\mathbf{F}_2)$$

has order 7). Using this element of order 7, we define an injective group homomorphism $\varphi : \mathbf{Z}/7 \to \mathrm{Aut}(\mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/2)$ as follows: let $y \in G$ have order 7, so that $\langle y\rangle$ is a Sylow 7-subgroup of G, and let $a, b, c \in G$ be such that the Sylow 2-subgroup of G is given by $S = \langle a\rangle \times \langle b\rangle \times \langle c\rangle$. Then define by $\varphi(y) = s$. We can easily determine that y acts on a, b, c as:

$$y.a = b \qquad y.b = bc \qquad y.c = a.$$

This gives a group $G = \mathbf{Z}/7 \ltimes_\varphi (\mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/2)$ of order 56 with a non-normal Sylow 7-subgroup. Moreover, G is unique up to isomorphism: indeed, $\mathbf{Z}/7$ is cyclic and any two nontrivial homomorphisms $\varphi_i : \mathbf{Z}/7 \to \mathrm{Aut}(\mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/2)$ for $i = 1, 2$ must map $\mathbf{Z}/7$ isomorphically to a Sylow 7-subgroup of $\mathrm{Aut}(\mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/2)$, as we have seen. But the Sylow 7-subgroups of $\mathrm{Aut}(\mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/2)$ are all conjugate so that $\varphi_1(K)$ and $\varphi_2(K)$ are conjugate subgroups. It follows from §5.5 Problem 6 that $\mathbf{Z}/7 \ltimes_{\varphi_1} (\mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/2) \simeq \mathbf{Z}/7 \ltimes_{\varphi_2} (\mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/2)$.

8. Construct a non-abelian group of order 75. Classify all groups of order 75.

Solution: Let G be any group of order $75 = 3 \cdot 5^2$. The number of Sylow 5-subgroups of G divides 3 and is 1 mod 5. Therefore, there is a unique Sylow 5-subgroup, $H \lhd G$. Similarly, the number of Sylow 3-subgroups of G is either 1 or 25. If there is a unique Sylow 3-subgroup $K \lhd G$ then $K \cap H = 1$ and

$KH = G$ by order considerations. It follows from HW 3, Problem 1 that $G \simeq K \times H$. But H is of order 5^2 and we have seen that every group of order p^2 is abelian. It follows that $G \simeq \mathbf{Z}/5 \times \mathbf{Z}/15$ or $G \simeq \mathbf{Z}/75$ and it is clear that these represent distinct isomorphism types. Now suppose that there are 25 Sylow 3-subgroups of G. Then G is non-abelian and since $G = HK$ for any Sylow 3-subgroup K, we must have $G \simeq K \ltimes_\varphi H$ for some $\varphi : K \to \mathrm{Aut}(H)$. Now as above, since $|H| = 25$ we have either $H \simeq \mathbf{Z}/25$ or $H \simeq \mathbf{Z}/5 \times \mathbf{Z}/5$. In the former case, $\mathrm{Aut}(H) \simeq (\mathbf{Z}/25)^\times$ so that $|\mathrm{Aut}(H)| = 20$ and there are no nontrivial homomorphisms from K into $\mathrm{Aut}(H)$ (since $K \simeq \mathbf{Z}/3$). Therefore, we must have $H \simeq \mathbf{Z}/5 \times \mathbf{Z}/5$ and $\mathrm{Aut}(H) \simeq \mathrm{GL}_2(\mathbf{F}_5)$. Recall, however, that we have computed $|\mathrm{GL}_2(\mathbf{F}_5)| = (5^2-1)(5^2-5) = 2^5 \cdot 3 \cdot 5$ so that any nontrivial homomorphism $\varphi : K \to \mathrm{Aut}(H)$ takes a generator, say y, of K to an element of order 3 in $\mathrm{Aut}(H)$ and hence maps K isomorphically to a Sylow 3-subgroup of $\mathrm{Aut}(H)$. By §5.5, Problem 6, since all Sylow 3-subgroups of $\mathrm{Aut}(H)$ are conjugate and $K = \langle y \rangle$ is cyclic, any two nontrivial homomorphisms $\varphi_i : K \to \mathrm{Aut}(H)$ for $i = 1, 2$ give isomorphic groups $K \ltimes_{\varphi_1} H \simeq K \ltimes_{\varphi_2} H$. Explicitly, we find that

$$\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{GL}_3(\mathbf{F}_5)$$

has order 3. Writing $H = \langle a \rangle \times \langle b \rangle$ we find that y acts on a, b as

$$y.a = a^{-1}b^{-1} \qquad\qquad y.b = a.$$

9. Show that the matrix

$$\begin{pmatrix} 0 & -1 \\ 1 & 4 \end{pmatrix} \in \mathrm{GL}_2(\mathbf{F}_{19})$$

has order 5. Use this matrix to construct a non-abelian group of order 1805 and give a presentation of this group. Classify all groups of order 1805.

Solution: Let $s = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 4 \end{smallmatrix}\right)$. Observe that s has characteristic polynomial $x^2 - 4x + 1$ and that over $\mathbf{F}_{19}$ one has the factorization

$$x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + 1) = (x-1)(x^2 - 4x + 1)(x^2 + 5x + 1)$$

so that, since any matrix satisfies its characteristic polynomial by the Cayley—Hamilton Theorem, we have $s^5 = 1$ and s has order dividing 5. Since $s \neq 1$, we see that s has order 5. Thus, we define a homomorphism $\varphi : \mathbf{Z}/5 \to \mathrm{Aut}(\mathbf{Z}/19 \times \mathbf{Z}/19)$ by $y \mapsto s$, where $\langle y \rangle \simeq \mathbf{Z}/5$ (i.e. y has order 5). If we let a, b be such that $\mathbf{Z}/19 \times \mathbf{Z}/19 \simeq \langle a \rangle \times \langle b \rangle$ then we have

$$y.a = b \qquad\qquad y.b = a^{-1}b^4.$$

Thus, we have a non-abelian group $G = \mathbf{Z}/5 \ltimes_\varphi (\mathbf{Z}/19 \times \mathbf{Z}/19)$ of order $5 \cdot 19^2 = 1805$, with presentation

$$\langle y, a, b : y^5 = a^{19} = b^{19} = 1,\ ab = ba,\ yay^{-1} = b,\ yby^{-1} = a^{-1}b^4 \rangle.$$

Now suppose that G is any group with $|G| = 1805$. Then the number of Sylow 19-subgroups of G is 1 (since it is 1 mod 19 and divides 5) and the number of Sylow 5-subgroups is 1 or 361. In the case that there is a unique Sylow 5-subgroup, then we have (just as in Problem 8) $G \simeq \mathbf{Z}/5 \times \mathbf{Z}/19 \times \mathbf{Z}/19$ or $G \simeq \mathbf{Z}/5 \times \mathbf{Z}/19^2$ and these isomorphism classes are clearly distinct. Otherwise, there are 361 Sylow 5-subgroups and we have $G \simeq \mathbf{Z}/5 \ltimes \mathbf{Z}/19^2$ or $G \simeq \mathbf{Z}/5 \ltimes (\mathbf{Z}/19 \times \mathbf{Z}/19)$. In the former case, since $|\mathrm{Aut}(\mathbf{Z}/19^2)| = |(\mathbf{Z}/19^2)^\times| = 2 \cdot 3^2 \cdot 19$ there are no nontrivial homomorphisms $\varphi : \mathbf{Z}/5 \to \mathrm{Aut}(\mathbf{Z}/19^2)$, and the semidirect product $G \simeq \mathbf{Z}/5 \ltimes \mathbf{Z}/19^2$ is a direct product. In the latter case, observe that $\mathrm{Aut}(\mathbf{Z}/19 \times \mathbf{Z}/19) \simeq \mathrm{GL}_2(\mathbf{F}_19)$, which is a group of order $(19^2-1)(19^2-19) = 2^4 \cdot 3^4 \cdot 5 \cdot 19$. Therefore, any nontrivial homomorphism $\varphi : \mathbf{Z}/5 \to \mathrm{Aut}(\mathbf{Z}/19 \times \mathbf{Z}/19)$ maps $\mathbf{Z}/5$ isomorphically to a Sylow 5-subgroup of $\mathrm{Aut}(\mathbf{Z}/19 \times \mathbf{Z}/19)$. Since all Sylow 5-subgroups of $\mathrm{Aut}(\mathbf{Z}/19 \times \mathbf{Z}/19)$ are conjugate and $\mathbf{Z}/5$ is cyclic, we apply §5.5 Problem 6 to determine that up to isomorphism, there is a unique non-abelian group of order 1805, namely, the one we determined above.

1. Let G be a finite p-group.

   (i) For every proper subgroup H in G, show that H is a proper subgroup of its normalizer.

Solution: We induct on the size of G. The statement is clear for $|G| = p$ since in this case any proper subgroup is trivial and G is abelian. Since G is a p-group, $Z(G)$ is nontrivial. If $Z(G) \not\leqslant H$ then there exists some $g \in Z(G) - H$, and certainly $g \in N_G(H)$ so that H is a proper subgroup of $N_G(H)$. Therefore, suppose $Z(G) \leqslant H$. We may further assume that $H \neq Z(G)$ since otherwise $N_G(H) = G$ and since H is a proper subgroup of G by hypothesis, it is a proper subgroup of $N_G(H)$. We are reduced to the case that $Z(G)$ is a proper subgroup of H. Then $H/Z(G)$ is a nontrivial proper subgroup of $G/Z(G)$ and by our induction hypothesis, since $|G/Z(G)| < |G|$, we have that $H/Z(G)$ is a proper subgroup of $N_{G/Z_(G)}(H/Z(G)) = N_G(H)Z(G)/Z(G)$. Since $Z(G) \leqslant H$ and $H/Z(G)$ is a *proper* subgroup of $N_G(H)Z(G)/Z(G)$, it follows that H is a proper subgroup of $N_G(H)$.

(ii) Deduce that there exists a solvability series for G in which one of the terms in actually H.

Solution: It is enough to show that there is a chain of subgroups of G of the form

$$H \lhd G^1 \lhd G^2 \lhd \ldots \lhd G^n = G. \qquad (1)$$

For since H is a p-group, it is solvable so there is a solvability series $1 \lhd H^1 \lhd H^1 \lhd \ldots \lhd H^m = H$. Moreover, G^{i+1}/G^i is a p-group. If it is cyclic, we are done. Otherwise, let $y \in Z(G^{i+1}/G^i)$ have order p (we know that G^{i+1}/G^i has nontrivial center since it is a p-group). Using the one-to-one (normality preserving) correspondence between subgroups of G^{i+1} containing G^i and subgroups of G^{i+1}/G^i, we deduce that there exists a normal subgroup $G' \lhd G^{i+1}$ containing G^i (normal since $y \in Z(G^{i+1}/G^i)$ and hence $\langle y \rangle \lhd G^{i+1}/G^i$) with $G'/G^i \simeq \mathbf{Z}/p$. Thus we have successfully refined our composition series. We continue by induction and are therefore reduced to showing that a series of the form (1) exists. By part (ii), we know that H is a proper subgroup of $N_G(H)$ and trivially, $H \lhd N_G(H)$. Therefore, set $G^1 = N_G(H)$. In general, let $G^i = N_G(G^{i-1})$. Then part (ii) tells us that G^i is a proper, normal subgroup of G^{i+1} whenever G^i is a proper subgroup of G. Since $|G|$ is finite, it follows that $G^n = G$ for some G and we have produced the requisite series.

(iii) Give an example of a non-trivial quotient situation G/H for which there does not exist a subgroup K in G with $K \to G/H$ an isomorphism (concretely, we can't "lift" G/H *as a group* back into G). Hint: think of cyclic groups.

Solution: Let $G = \mathbf{Z}$ and $H = n\mathbf{Z}$ considered as additive groups, with $n > 1$. If we had an isomorphism $K \to \mathbf{Z}/n\mathbf{Z}$ for some $K < \mathbf{Z}$ then there would be a nonzero integer of finite order. Clearly this is absurd.