Homework Assignment 11

Due Friday, April 22

This assignment will fill in many details from lecture, and do a few hands on classifications. To begin we will confirm that the semidirect product is indeed a group. First recall the definition.

Definition 1. *Let H, K be groups, and $\varphi : K \to \mathrm{Aut}(H)$ a group homomorphism. Denote the induced action of K on H by:*

$$k \cdot h = \varphi(k)(h).$$

The semidirect product of H and K with respect to φ is the set $H \rtimes K = \{(h, k) : h \in H, k \in K\}$, where multiplication is defined by the rule:

$$(h_1, k_1)(h_2, k_2) = (h_1(k_1 \cdot h_2), k_1k_2).$$

1. Let's make sure that $H \rtimes K$ is a group.

   (a) Show that $(1, 1) \in H \rtimes K$ is the identity. (Remember you have to check both sides).

   Proof. Fix $h \in H$ and $k \in H$. Then we check,

   $$(1, 1)(h, k) = (1(1 \cdot h), 1k) = (h, k).$$

   On the other hand:

   $$(h, k)(1, 1) = (h(k \cdot 1), k1) = (h, k),$$

   where we remark that $k \cdot 1 = 1$ because K acts *by automorphisms* (i.e. $x \mapsto k \cdot x$ is not merely a bijection, but also a homomorphism which in particular sends 1 to 1 [by HW3 Problem 4a]). □

   (b) Show that $(h, k)^{-1} = (k^{-1} \cdot h^{-1}, k^{-1})$. (As above, you have to check both sides).

   Proof. We check both directly:

   $$\begin{aligned}(h,k)(k^{-1} \cdot h^{-1}, k^{-1}) &= (h(k \cdot (k^{-1} \cdot h^{-1})), kk^{-1}) \\ &= (h(kk^{-1} \cdot h^{-1})), 1) \\ &= (h(1 \cdot h^{-1}), 1) \\ &= (hh^{-1}, 1) \\ &= (1, 1).\end{aligned}$$

   For the other side, we remark that because K acts by automorphisms, we have that for each $\ell \in K$, we have $(\ell \cdot x)(\ell \cdot y) = \ell \cdot (xy)$ (because $x \mapsto \ell \cdot x$ is a homomorphism). In particular

   $$\begin{aligned}(k^{-1} \cdot h^{-1}, k^{-1})(h, k) &= ((k^{-1} \cdot h^{-1})(k^{-1} \cdot h), k^{-1}k) \\ &= (k^{-1} \cdot (h^{-1}h), 1) \\ &= (k^{-1} \cdot 1, 1) \\ &= (1, 1).\end{aligned}$$

   □

(c) Prove that multiplication is associative.

Proof. We consider $h_1, h_2, h_3 \in H$ and $k_1, k_2, k_3 \in K$. We passing from line 2 to 3 that K acts by automorphism. Then:

$$\begin{aligned}
((h_1,k_1)(h_2,k_2))\,(h_3,k_3) &= (h_1(k_1 \cdot h_2), k_1k_2)(h_3,k_3) \\
&= (h_1(k_1 \cdot h_2)(k_1k_2 \cdot h_3), k_1k_2k_3) \\
&= (h_1(k_1 \cdot (h_2(k_2 \cdot h_3)), k_1k_2k_3) \\
&= (h_1,k_1)(h_2(k_2 \cdot h_3), k_2k_3) \\
&= (h_1,k_1)\,((h_2,k_2)(h_3,k_3))\,.
\end{aligned}$$

□

2. Consider again the setup of Definition 1. Let's prove some basic properties about $G = H \rtimes K$.

(a) Show that the subset $\{(h,1) : h \in H\} \subseteq G$ is a subgroup isomorphic to H. Similarly, show that $\{(1,k) : k \in K\} \subseteq G$ is a subgroup isomorphic to K. In what follows we identify H and K with these subgroups, and write $H, K \leq G$.

Proof. Consider the map $\varphi : H \to H \rtimes K$ defined by the rule $\varphi(h) = (h,1)$. We observe it is a homomorphism because:

$$\varphi(h)\varphi(h') = (h,1)(h',1) = (h(1 \cdot h'),1) = (hh',1) = \varphi(hh').$$

It is also injective since $\varphi(h) = (1,1)$ precisely when $h = 1$. Therefore by the first isomorphism theorem and HW4 Problem 4(b) we have:

$$H \cong \operatorname{im}\varphi = \{\varphi(h) : h \in H\} = \{(h,1) : h \in H\} \leq G.$$

Almost (but not quite) symmetrically we next consider the map $\psi : K \to H \rtimes K$ given by the rule $\psi(k) = (1,k)$. This is a homomorphism because:

$$\psi(k)\psi(k') = (1,k)(1,k') = (k \cdot 1, kk') = (1,kk') = \psi(kk'),$$

where the second to last equality crucially uses that K acts by automorphisms. Injectivity follows similarly to above, $\psi(k) = (1,1)$ precisely when $k = 1$, so that the first isomorphism theorem and HW4 Problem 4(b):

$$K \cong \operatorname{im}\psi = \{\psi(k) : k \in K\} = \{(1,k) : k \in K\} \leq G.$$

□

(b) Prove that $H \cap K = \{1_G\}$.

Proof. Under the identification above we have:

$$H \cap K = \{(h,1) : h \in H\} \cap \{(1,k) : k \in K\} = \{(1,1)\}.$$

□

(c) Show that $H \trianglelefteq G$ and $G/H \cong K$.

Proof. Define a function $\pi : G \to K$ given by the rule $\pi(h,k) = k$. Let's observe this is a homomorphism:

$$\pi(h_1,k_1)\pi(h_2,k_2) = k_1k_2,$$

while

$$\pi\Big((h_1,k_1)(h_2,k_2)\Big) = \pi\Big(h_1(k_1\cdot h_2), k_1k_2\Big) = k_1k_2.$$

We then see π is surjective since any $k = \pi(1,k)$. Finally we compute the kernel: $\pi(h,k) = 1$ if and only if $k = 1$, if and only if $(h,k) = (h,1) \in H$. Therefore $\ker\pi = H$, and so H is normal since it is a kernel. Finally, the first isomorphism theorem gives us that

$$K \cong G/\ker\pi = G/H.$$

□

In HW 10 Problem 5 we proved the *Recognition Theorem for Direct Products* (HW10 Theorem 3). There is an analogous result for semidirect products, and in fact you already did most of the work. Let's state the result.

Theorem 2 (Recognition Theorem for Semidirect Products)**.** *Suppose G is a group and $H, K \leq G$ are subgroups. Suppose that $H \trianglelefteq G$ is normal, and that $H \cap K = 1$. Then*

$$HK \cong H \rtimes_\varphi K,$$

where $\varphi : K \to \mathrm{Aut}(H)$ corresponds to the action of K on H by conjugation (in G). In particular, if $HK = G$ then $G \cong H \rtimes_\varphi K$.

3. Prove Theorem 2 by showing that function $H \rtimes_\varphi K \to HK$ defined by the rule $(h,k) \mapsto hk$ is an isomorphim. (*Note:* Bijectivity should follow from HW10 Problem 5(a), so the main verification is that it is a homomorphism).

   Proof. Bijectivity follows identically to HW10 Probem 5(c). We reproduce the proof here (but don't require it). Call the map $\Phi(h,k) = hk$. Surjectivity is immediate, as any hk in the target is the image of (h,k). As for injectivity, let $\Phi(h,k) = \Phi(h',k')$, so that $hk = h'k'$. Using that $H \cap K = \{1\}$, HW10 Problem 5(a) tells us that there is a unique way to write hk as an element of H times one of K, so that $h = h'$ and $k = k'$.

   It remains to show that Φ is a homomorphism. Notice that in $H \rtimes K$ we have:

   $$(h_1,k_1)(h_2,k_2) = (h_1(k_1\cdot h_2), k_1k_2) = (h_1k_1h_2k_1^{-1}, k_1k_2),$$

   because the action of K on H is that by conjugation in HK. Then after applying Φ we get:

   $$\Phi\Big((h_1,k_1)(h_2,k_2)\Big) = (h_1k_1h_2k_1^{-1})(k_1k_2) = (h_1k_1)(h_2k_2) = \Phi(h_1,k_1)\Phi(h_2,k_2),$$

   completing the proof. □

4. A lot of studying semidirect products comes down to enumerating and classifying homomorphisms.

(a) Show that giving a homomorphism $Z_n \to G$ is the same as selecting an element $g \in G$ with $|g|$ dividing n. That is, give a bijection between the following sets:

$$\left\{ \begin{array}{c} \text{Homomorphisms} \\ Z_n \to G \end{array} \right\} \Longleftrightarrow \left\{ \begin{array}{c} \text{Elements } g \in G \\ \text{where } |g| \text{ divide } n \end{array} \right\}$$

Proof. Fix once and for all a generator x of Z_n. Then given a map $\varphi : Z_n \to G$, we know that $g = \varphi(x) \in G$ has order dividing $|x| = n$ (HW3 Probelem 4(c)). Conversely, given $g \in G$ of order dividing n, the map $\psi : x^i \mapsto g^i$ is a homomorphism from $Z_n \to G$. One readily checks that these are inverse constructions. □

(b) If p is prime show that giving a *nontrivial* map $Z_p \to G$ is the same as choosing an element of order p in G. (Note: the trivial map is the one that sends every element to the identity of G).

Proof. In part (a) we saw that a map $Z_p \to G$ is the same as an element of G whose order divides p. The trivial map corresponds to 1_G, so all other maps correspond to elements of order p. □

(c) Show that giving a homomorphism $Z_{n_1} \times \cdots \times Z_{n_r} \to G$ is the same as chosing elements $g_1, \cdots, g_r \in G$ such that all the g_i commute with eachother and each $|g_i|$ divides n_i.

Proof. This is essentially identical to part (a). Fix generators x_i of Z_{n_1}. Given a homomorphism φ we let $g_i = \varphi(x_i)$ and remark that its order must divide $|x_i| = n_i$ (again HW3 4(c)). Furthermore, we notice that:

$$g_i g_j = \varphi(x_i)\varphi(x_j) = \varphi(x_i x_j) = \varphi(x_j x_i) = \varphi(x_j)\varphi(x_i) = g_j g_i,$$

so that they commute. Conversely, given such g_i, we define ψ on the generators of $Z_{n_1} \times \cdots \times Z_{n_r}$ via the rule

$$\psi(x_1^{j_1}, \cdots, x_r^{j_r}) = g_1^{j_1} \cdots g_r^{j_r},$$

noting that ψ is a homomorphism precisely because the g_i commute and have order dividing x_i. □

(d) Suppose G is abelian and p is prime. Describe the set of homomorphisms $Z_p \times Z_p \to G$ as a subset of $G \times G$.

Proof. By part (c) this should correspond to pairs $(a, b) \in G \times G$ such that $a^p = b^p = 1$. We remark that actually a subgroup of $G \times G$, called the *p-torsion subgroup*. □

Any homomorphism $\varphi : K \to \operatorname{Aut} H$ allows us to build a semidirect product $H \rtimes_\varphi K$. An interesting question is when different maps give us isomorphic semidirect products. In class we stated and used a special case of the following lemma.

Lemma 3. *Let $\varphi, \psi : K \to \operatorname{Aut} H$ be two homomorphisms, and suppose they differ by an automorphism of K. That is, suppose there is some $\gamma \in \operatorname{Aut}(K)$ such that $\psi \circ \gamma = \varphi$:*

$$\begin{tikzcd} K \arrow[d, "\gamma"'] \arrow[dr, "\varphi"] & \\ K \arrow[r, "\psi"'] & \operatorname{Aut} H \end{tikzcd}$$

Then $H \rtimes_\varphi K \cong H \rtimes_\psi K$.

One could ask if this is the only thing that could allow different φ to give different semidirect products. The answer would be no, as the following lemma shows.

Lemma 4. *Let $\varphi, \psi : K \to \operatorname{Aut} H$ be two homomorphisms, and suppose they are conjugate in $\operatorname{Aut} H$. Explicitely, suppose there is some $\alpha \in \operatorname{Aut} H$, corresponding to the inner automorphism $\sigma_\alpha : \beta \mapsto \alpha\beta\alpha^{-1}$, and suppose that $\psi = \sigma_\alpha \circ \varphi$:*

$$\begin{tikzcd} & \operatorname{Aut} H \arrow[d, "\sigma_\alpha"] \\ K \arrow[ur, "\varphi"] \arrow[r, "\psi"'] & \operatorname{Aut} H \end{tikzcd}$$

Then $H \rtimes_\varphi K \cong H \rtimes_\psi K$.

5. Lemmas 3 and 4 say that if we alter φ by an automorphism of K, or an inner automorphism of $\operatorname{Aut} H$, (or both), we don't change the semidirect products. Let's prove this.

   (a) Consider the setup of Lemma 3. Show that the map:

$$\begin{array}{rcl} H \rtimes_\varphi K & \longrightarrow & H \rtimes_\psi K \\ (h,k) & \mapsto & (h, \gamma(k)) \end{array}$$

   is an isomorphism, thereby proving the lemma.

   Proof. Call the map we are studying Φ. Since γ is bijective, so is Φ. So it suffices to show that Φ is a homomorphism. Fix $(h_i, k_i) \in H \rtimes_\varphi K$ for $i = 1, 2$.

$$\begin{aligned} \Phi(h_1,k_1)\Phi(h_2,k_2) &= \Big(h_1, \gamma(k_1)\Big)\Big(h_2, \gamma(k_2)\Big) \\ &= \Big(h_1(\psi(\gamma(k_1))(h_2)), \gamma(k_1)\gamma(k_2)\Big) \\ &= \Big(h_1(\varphi(k_1)(h_2)), \gamma(k_1k_2)\Big) \\ &= \Phi\Big(h_1(\varphi(k_1)(h_2)), k_1k_2\Big) \\ &= \Phi\Big((h_1,k_1)(h_2,k_2)\Big), \end{aligned}$$

   and the result follows. $\square$

(b) Consider the setup of Lemma 4. Show that the map:

$$\begin{array}{ccc} H \rtimes_{\varphi} K & \longrightarrow & H \rtimes_{\psi} K \\ (h, k) & \mapsto & (\alpha(h), k) \end{array}$$

is an isomorphism, thereby proving the lemma. (Notice that $\alpha \in \operatorname{Aut} H$ is an automorphism of H, wheras σ_α is an automorphism of $\operatorname{Aut} H$, given by conjugation by α. In unweildy notation, this says $\sigma_\alpha \in \operatorname{Aut}(\operatorname{Aut} H)$.)

Proof. Call the map we are studying Ψ. Since α is bijective, so is Ψ, so it suffices to show that Ψ is an automorphism. Fix $(h_i, k_i) \in H \rtimes_{\varphi} K$ for $i = 1, 2$.

$$\begin{aligned} \Psi(h_1, k_1)\Psi(h_2, k_2) &= \Big(\alpha(h_1), k_1\Big)\Big(\alpha(h_2), k_2\Big) \\ &= \Big(\alpha(h_1)(\psi(k_1)(\alpha(k_2)), k_1k_2\Big) \\ &= \Big(\alpha(h_1)(\sigma_\alpha(\varphi((k_1)))(\alpha(k_2)), k_1k_2\Big) \\ &= \Big(\alpha(h_1)(\alpha\varphi(k_1)\alpha^{-1})(\alpha(h_2)), k_1k_2\Big) \\ &= \Big(\alpha(h_1)\alpha(\varphi(k_1)(h_1)), k_1k_2\Big) \\ &= \Big(\alpha(h_1(\varphi(k_1)(h_1)), k_1k_2\Big) \\ &= \Psi\Big(h_1(\varphi(k_1)(h_1)), k_1k_1\Big) \\ &= \Psi\Big((h_1, k_1)(h_2, k_2)\Big). \end{aligned}$$

□

(c) Now suppose $\varphi, \psi : K \to \operatorname{Aut} H$ are two homomorphisms, and suppose there is an automorphism $\gamma \in \operatorname{Aut} K$ and an inner automorphism $\sigma \in \operatorname{Inn}(\operatorname{Aut}(H))$ such that the following diagram commutes:

$$\begin{tikzcd} K \arrow[r, "\varphi"] \arrow[d, "\gamma"'] & \operatorname{Aut} H \arrow[d, "\sigma"] \\ K \arrow[r, "\psi"] & \operatorname{Aut} H. \end{tikzcd}$$

That is, $\sigma \circ \varphi = \psi \circ \gamma$. Then $H \rtimes_{\varphi} K \cong H \rtimes_{\psi} K$. (Hint: This should follow formally from Lemmas 3 and 4, so you shouldn't have to do any lengthy computations).

Proof. We give the function $\sigma \circ \varphi = \psi \circ \gamma$ the name $\xi : K \to \operatorname{Aut} H$. That is, ξ fits into the following diagram:

$$\begin{tikzcd} K \arrow[r, "\varphi"] \arrow[d, "\gamma"'] \arrow[dr, dotted, "\xi"'] & \operatorname{Aut} H \arrow[d, "\sigma"] \\ K \arrow[r, "\psi"'] & \operatorname{Aut} H. \end{tikzcd}$$

By part (b), we know that

$$H \rtimes_{\varphi} K \cong H \rtimes_{\xi} K,$$

and by part (a) we know that

$$H \rtimes_{\xi} K \cong H \rtimes_{\psi} K.$$

Combining these two gives the result. $\square$

6. We've seen 5 groups of order 12: $Z_{12}, Z_6 \times Z_2, D_{12}, A_4$, and a nontrivial semidirect product $Z_3 \rtimes Z_4$ where the generator of Z_4 acts on Z_3 by inverting elements. Let's prove this is all of them!

   (a) Let G be a group of order 12. Show that if $G \ncong A_4$, then $G \cong Q \rtimes P$ where P is a Sylow 2-subgroup and Q is a Sylow 3-subgroup. (*Hint*: **(Sylow 3)** and the Theorem 2 should help).

   Proof. Let $P \leq G$ be a Sylow 2-subgroup (of order 4), and Q a Sylow 3-subgroup (of order 3). By HW9 Problem 3(b), if Q isn't normal, then $G \cong A_4$, so we may assume that $Q \trianglelefteq G$. Since $Q \cap P$ have order dividing both 3 and 4, so it must be trivial. Finally, we see that:

$$|QP| = \frac{|Q| \cdot |P|}{|Q \cap P|} = 12,$$

   so that $QP = G$. Therefore Theorem 2 shows that $G \cong Q \rtimes P$. $\square$

   (b) Show that there is only one abelian and one nonabelian semidirect product $Z_3 \rtimes Z_4$ up to isomorphism.

   Proof. For every $\varphi : Z_4 \to \mathrm{Aut}(Z_3)$ we get a semidirect product group $Z_3 \rtimes_{\varphi} Z_4$. Notice that $\mathrm{Aut}(Z_3) \cong (\mathbb{Z}/3\mathbb{Z})^{\times} \cong Z_2$, so this boils down to classifying maps $\varphi : Z_4 \to Z_2$. Let $Z_4 = \langle z \rangle$ and $Z_2 = \langle y \rangle$. By 4(a), the φ correspond to elements of Z_2 whose order divide 4, which correspond to choosing the image of z. In particular, we have

$$\begin{aligned} \varphi_0 : Z_4 &\to Z_2 \\ z &\mapsto 1 \end{aligned} \qquad \text{and} \qquad \begin{aligned} \varphi_1 : Z_4 &\to Z_2 \\ z &\mapsto x \end{aligned}$$

   In particular, there are at most 2 semidirect products: $G_i = Z_3 \rtimes_{\varphi_i} Z_4$ for $i = 0, 1$. If $i = 0$ then φ is the trivial map, and the semidirect product corresponds to the direct product giving

$$G_0 = Z_3 \rtimes_{\varphi_0} Z_4 \cong Z_3 \times Z_4 \cong Z_{12}.$$

   We proved in class that any nontrivial semidirect product is nonabelian, so this shows G_0 is the unique abelian case, and that G_1 is nonabelian. Since there are no other semidirect products, this exhaustive list completes our proof. $\square$

   (c) Show that there is only one abelian and one nonabelian semidirect prodcut $Z_3 \rtimes (Z_2 \times Z_2)$ up to isomorphism. (You might need Lemma 3).

   Proof. As above, this boils down to classifying maps:

$$\psi : (Z_2 \times Z_2) \to \mathrm{Aut}(Z_3) \cong Z_2.$$

Let $Z_2 \times Z_2 = \langle a \rangle \times \langle b \rangle$ and let the right side $Z_2 = \langle x \rangle$. By 4(c), classifying such ψ this boils down to choosing 2 elements of Z_2, corresponding to picking the images of a and b. There are four options, which we will denote by $\psi_{j,k}$ for $j, k \in \{0, 1\}$.

$$\psi_{0,0} : \begin{array}{l} a \mapsto 1 \\ b \mapsto 1 \end{array} \qquad \psi_{1,0} : \begin{array}{l} a \mapsto x \\ b \mapsto 1 \end{array}$$

$$\psi_{0,1} : \begin{array}{l} a \mapsto 1 \\ b \mapsto x \end{array} \qquad \psi_{1,1} : \begin{array}{l} a \mapsto x \\ b \mapsto x \end{array}$$

We let $G_{j,k} = Z_3 \rtimes_{\psi_{j,k}} (Z_2 \times Z_2)$.

Case A: $j = k = 0$

In this case $\psi_{0,0}$ is trivial so arguing as in part (b) we have the unique abelian semidirect product of this form:

$$G_{0,0} \cong Z_3 \times (Z_2 \times Z_2) \cong Z_6 \times Z_2.$$

Case B: j, k **not both** 0

We claim that in this case all the $G_{j,k}$ are isomorphic. We remark that

$$Z_2 \times Z_2 \cong \langle a \rangle \times \langle b \rangle \cong \langle a \rangle \times \langle ab \rangle \cong \langle ab \rangle \times \langle b \rangle,$$

and each nontrivial $\psi_{j,k}$ takes 2 generators to x and the third to 1. But $\mathrm{Aut}(Z_2 \times Z_2) = GL_2(\mathbb{F}_2)$ includes all the *change of basis* matrices which takes a pair of generators to any other pair of generators. In particular, if we fix any nontrivial $\psi_{j,k}$ and view $Z_2 \times = \langle g \rangle \times \langle h \rangle$ as generated by g and h for the two generators sent to x (i.e., where $\psi_{j,k}(g) = \psi_{j,k}(h) = x$ and $\psi_{j,k}(gh) = 1$) then there exists some $\eta \in \mathrm{Aut}(Z_2 \times Z_2)$ where $\eta(a) = g$ and $\eta(b) = h$. That is, we have the following:

$$\begin{tikzcd}
Z_2 \times Z_2 \arrow[d, "\eta"] \arrow[dr, "\psi_{1,1}"] & \\
 & \mathrm{Aut}(Z_3) \cong Z_2 \\
Z_2 \times Z_2 \arrow[ur, "\psi_{j,k}"'] &
\end{tikzcd}$$

By Lemma 3 this shows $G_{1,1} \cong G_{i,j}$, so that all three nontrivial $G_{i,j}$'s must be isomorphic. □

(d) Put together parts (a)-(c) to deduce that there are exactly 5 groups of order 12 up to isomorphism. Of the semidirect products classified in parts (b) and (c), which one corresponds to D_{12}?

Proof. We will prove that D_{12} is isomorphic to the nonabelian group from part (c). We first observe that $D_{12} \ncong G_0$ and $D_{12} \ncong G_{0,0}$, because those two groups are abelian and

D_{12} is not.

Next we observe that $D_{12} \ncong A_4$ (one can also quote that we observed this in class). This is because A_4 has a unique Sylow 2-subgroup given by $\{(1), (12)(34), (13)(24), (14)(23)\}$, which is normal since it consists precisely of the identity and the entire 2-2 cycle type. On the other hand, $P = \{1, r^3, s, sr^3\}$, is a Sylow 2-subgroup of D_{12}, but $rsr^{-1} = sr^4 \notin P$, so that $P \trianglelefteq D_{12}$, and therefore has more than one Sylow 2-subgroup.

Finally we observe that $D_{12} \ncong G_1$. Indeed, the subgroup P from the previous paragraph is isomorphic to $Z_2 \times Z_2$ (every element squares to 1!), whereas the Sylow 2-subgroup of G_1 is isomorphic to Z_4.

Therefore $D_{12} \cong G_{j,k}$ for j, k not both zero. □

7. In this problem we classify all groups of order 75 up to isomorphism. (There should be 3 total).

(a) List all the abelian groups of order 75 using the fundamental theorem of finite abelian groups.

Proof. Notice $75 = 3 * 5^2$. Therefore, these decompose into elementary divisor form as:

$$Z_3 \times Z_{25} \qquad \text{and} \qquad Z_3 \times Z_5 \times Z_5.$$

In invariant factor form these correspond to Z_{75} and $Z_{15} \times Z_5$ respectively. □

(b) Prove that a group of order 75 is isomorphic to $P \rtimes Q$ where P is a Sylow 5-subgroup and Q is a Sylow 3-subgroup.

Proof. Let $|G| = 75 = 3 \cdot 5^2$. By Sylow III we know $n_5 \in \{1, 6, 11, \cdots\}$ and that n_5 divides 3. Therefore $n_5 = 1$ and so we can fix the *unique* Sylow 5-subgroup P, which by necessity is normal (HW9 Problem 1). Let Q be any Sylow 3-subgroup. Then $P \cap Q = \{1\}$ by Lagrange's theorem. We then compute:

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{25 \cdot 3}{1} = 75 = |G|.$$

Therefore $PQ = G$. Theorem 2 (or Problem 3) now gives the result.. □

(c) Prove that if a group of order 75 has a *cyclic* Sylow 5-subgroup, then it is abelian.

Proof. By part (b), we know $G \cong P \rtimes_\varphi Q$ for some map $\varphi : Q \to \mathrm{Aut}(P)$. By assumption, $P \cong Z_{25}$, and by TH1 Problem 4 we know $Q \cong Z_3$. Therefore we may identify φ with map

$$Z_3 \to \mathrm{Aut}(Z_{25}) \cong Z_{20}.$$

By 4(a) this corresponds to selecting an element in Z_{20} whose order divides 3. By Lagrange's theorem this can only be the identity element, so in fact φ is the trivial map. Therefore $G \cong Z_{25} \times Z_3 \cong Z_{75}$ which is abelian. □

(d) Show that there is a unique nonabelian group of order 75 up to isomorphism. (*Hint:* Show that 3 is a maximal 3-divisor of $|GL_2(\mathbb{F}_5)|$. Then use Sylow's theorems and 5(c).)

Proof. By part (c), to be nonabelian we must have $P \cong Z_5 \times Z_5$. Therefore we must study nontivial maps

$$\psi : Z_3 \longrightarrow \mathrm{Aut}(Z_5 \times Z_5) \cong GL_2(\mathbb{F}_5).$$

In HW 6 problem 7(d) we computed:

$$|GL_2(\mathbb{F}_5)| = 5^4 - 5^3 - 5^2 + 5 = 480 = 3 * 160.$$

Since $3|480$ then by Cauchy's theorem there exists an element $M \in GL_2(\mathbb{F}_3)$ of order 3. If y is a generator of Z_3, then we let $\varphi(y) = M$ and get a nonabelian group

$$G_\varphi = (Z_5 \times Z_5) \rtimes_\varphi Z_3$$

of order 75. In fact, any such group comes from choosing some N of order 3 in $|GL_2(\mathbb{F}_5)|$ and letting $\psi : y \mapsto N$ and building G_ψ as above. We finish the proof by showing $G_\psi \cong G_\varphi$.

Since $3 \not| 160$, we know $\langle M \rangle$ and $\langle N \rangle$ are both Sylow 3-subgroups of $GL_2(\mathbb{F}_5)$. Therefore they are conjugate. That is, there is some $\alpha \in GL_2(\mathbb{F}_5)$ such that

$$\alpha \langle M \rangle \alpha^{-1} = \langle N \rangle.$$

Denote by $\sigma_\alpha \in \mathrm{Inn}(GL_2(\mathbb{F}_5))$ the associated inner automorphism. In particular, we see that $\sigma(M)$ is either N or N^2. Define $\gamma : Z_3 \to Z_3$ by the following rule. If $\sigma_\alpha(M) = N$ then γ is the identity, and if $\sigma_\alpha(M) = N^2$ then $\gamma : y \mapsto y^2$. In either case, $\gamma \in \mathrm{Aut}(Z_3)$. In particular, we have the following commutative diagram:

$$\begin{tikzcd}
Z_3 \arrow[r, "\varphi"] \arrow[d, "\gamma"'] & GL_2(\mathbb{F}_5) \arrow[d, "\sigma_\alpha"] \\
Z_3 \arrow[r, "\psi"'] & GL_2(\mathbb{F}_5),
\end{tikzcd}$$

where the vertical maps are automorphisms, and the right one is even inner. Applying Problem 5(c) immediately implies:

$$G_\varphi = (Z_5 \times Z_5) \rtimes_\varphi Z_3 \cong (Z_5 \times Z_5) \rtimes_\psi Z_3 = G_\psi,$$

and so we are done. $\square$