2. (b) (5 points) Let \( \phi \) be any element in \( Aut_G(G/H) \), then \( \phi(H) = xH \) for some coset \( xH \) of \( H \). Note that \( \phi \) is completely determined by \( x \) in the sense that \( \phi(gH) = g\phi(H) = gxH \) for any \( g \in G \) (the first equality holds because \( \phi \) is a homomorphism of \( G \)-sets.) Thus we can denote any element in \( Aut_G(G/H) \) by \( \phi_x \) for some \( x \in G \).

Let \( f : Aut_G(G/H) \to N_G(H)/H \) be defined by \( f(\phi_x) = xH \). We first show that \( f \) is well-defined by showing (1) \( x \in N_G(H) \) and (2) \( f(\phi_x \circ \phi_y) = xy \). For (1), note that by definition \( \phi_x \) is injective, so \( \phi_x(gH) = \phi_x(H) \) implies \( g \in H \). But the equality condition also implies \( gxH = g\phi_x(H) = xH \), i.e. \( x^{-1}gx \in H \), so \( g \in xHx^{-1} \) and we have \( H \subseteq xHx^{-1} \). On the other hand, for any \( h \in H \), we have \( hxH = \phi_x(hH) = \phi_x(H) = xH \), so \( h \in x^{-1}Hx \), which implies \( H \subseteq x^{-1}Hx \). Hence we conclude \( Hx = xH \), i.e. \( x \in N_G(H) \). (2) is straightforward: for any \( gH \in G/H \), \( \phi_x \circ \phi_y(gH) = \phi_x(gy^{-1}H) = gy^{-1}x^{-1}H = g(xy)^{-1}H \).

\( f \) is surjective because by an reverse argument of (1), any \( x \in N_G(H) \) gives an automorphism of \( G/H \) as a \( G \)-set. \( f \) is injective because \( f(\phi_x) = H \Rightarrow xH = H \Rightarrow x \in H \).

3. (a) (5 points) By the hint we see that \( \tau \) must give bijections between \( \{1, 2\} \) and \( \{1, 2\} \) or \( \{3, 4\} \) and \( \{1, 2\} \) or \( \{3, 4\} \); and \( \{5, 6, 7\} \) and \( \{5, 6, 7\} \). Thus \( \tau \in \langle (1, 2), (3, 4), (1, 4), (2, 3), (5, 6, 7) \rangle \), in which there are 24 elements.

3. (b) (5 points) Let \( G \) be a group with \( p^2 \) elements, then the order of any element must be 1, \( p \) or \( p^2 \). If there exits some \( g \in G \) with \( o(g) = p^2 \), then \( \langle g \rangle \subseteq G \) and \( |\langle g \rangle| = p^2 \), so \( G = \langle g \rangle \cong \mathbb{Z}/p^2\mathbb{Z} \).

If no element of \( G \) has order \( p^2 \), then all nontrivial elements of \( G \) have order \( p \). Let \( g \in G - \{e\} \), then \( G - \{e\} - \langle g \rangle \neq \emptyset \) as \( p^2 - p - 1 > 0 \) for any integer prime \( p \). Let \( h \in G - \{e\} - \langle g \rangle \). Then the map \( \langle g \rangle \times \langle h \rangle \to G \) given by \( (g^a, h^b) \mapsto g^ah^b \) gives an isomorphism. To show this, it suffices to show injectivity, which is true because \( g^ah^b = e \Rightarrow a = b = 0 \) since \( g \) and \( h \) are independent.

5. (10 points) It suffices to show that there are exactly two semi-direct products \( \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z} \) arising from group homomorphisms \( \mathbb{Z}/p\mathbb{Z} \to Aut(\mathbb{Z}/q\mathbb{Z}) = (\mathbb{Z}/q\mathbb{Z})^\times \). It is shown in class that from the trivial homomorphism we get the direct product \( \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \), so we only consider the case of nontrivial homomorphisms.

Since \( p\mid q - 1 \), \( (\mathbb{Z}/q\mathbb{Z})^\times \) has a subgroup of order \( p \). Giving a homomorphism between cyclic groups
amounts to specifying a generator of the target group, so there are $p - 1$ nontrivial homomorphisms $\phi : \mathbb{Z}/p\mathbb{Z} \to (\mathbb{Z}/q\mathbb{Z})^\times$. We show that the semidirect products that arise from any such $\phi, \psi$ are isomorphic. Let $f : \mathbb{Z}/p\mathbb{Z} \rtimes_\phi \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \rtimes_\psi \mathbb{Z}/q\mathbb{Z}$ be given by $f((a, b)) = (a, \psi^{-1}\phi(b))$. The desired properties follow from the fact that $\psi, \phi$ are injective homomorphisms and are straightforward to check.