1. (a) Homomorphism. $\text{Ker}(\varphi) = n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$. Onto but not 1-1.

   (b) Not a homomorphism unless $G$ is abelian. This is because $\varphi(ab) = (ab)^{-1} = b^{-1}a^{-1}$ which may not be equal to $\varphi(a)\varphi(b) = a^{-1}b^{-1}$.

   (c) Homomorphism. $\text{Ker}(\varphi) = \{e\}$. Onto and 1-1 (every element has a unique inverse).

   (d) Homomorphism. $\text{Ker}(\varphi) = \mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$. Onto but not 1-1.

   (e) Homomorphism. $\text{Ker}(\varphi) = \{x \in G \mid x^n = e\}$ (elements in $G$ whose order divides $n$). If $(n, |G|) = 1$, then $\varphi$ is onto and 1-1. Otherwise $\varphi$ is neither onto nor 1-1.

2. If $x, y \in \varphi(G)$, then we can find $x_g, y_g \in G$ such that $\varphi(x_g) = x$ and $\varphi(y_g) = y$. Thus $xy = \varphi(x_g)\varphi(y_g) = \varphi(x_g y_g)$. Since $G$ is a group, we have $x_g y_g \in G$ and hence $xy = \varphi(x_g y_g) \in \varphi(G)$. Similarly, we have $x^{-1} = (\varphi(x_g))^{-1} = \varphi({x_g}^{-1}) \in \varphi(G)$ since ${x_g}^{-1} \in G$. Finally, note that $e = \varphi(e) \in \varphi(G)$.

3. Suppose $\varphi$ is an monomorphism. Then $\varphi(x) = \varphi(y) \Rightarrow x = y$. If $x \in \text{Ker}(\varphi)$, we have $\varphi(x) = \varphi(e) = e$ which implies $x = e$. Hence $\text{Ker}(\varphi) \subset \{e\}$ and since $e \in \text{Ker}(\varphi)$, we have $\text{Ker}(\varphi) = \{e\}$.

   Suppose $\text{Ker}(\varphi) = \{e\}$. Let $x, y \in G$ be such that $\varphi(x) = \varphi(y)$. We have $\varphi(x)\varphi(y)^{-1} = e$ which implies $\varphi(xy^{-1}) = e$. Since $\text{Ker}(\varphi) = \{e\}$, we have $xy^{-1} = e$ which is equivalent to $x = y$. Hence $\varphi$ is injective.

4. Let $x', y' \in G'$. Since $\varphi$ is surjective, we can find $x, y \in G$ such that $\varphi(x) = x'$ and $\varphi(y) = y'$. Since $G$ is abelian, we have $xy = yx$. Then

$$x'y' = \varphi(x)\varphi(y) = \varphi(xy) = \varphi(yx) = \varphi(y)\varphi(x) = y'x',$$

   and hence $G'$ is abelian.

5. If $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in G_1 \times G_2$, then

$$\begin{aligned}
\Big((x_1, y_1)(x_2, y_2)\Big)(x_3, y_3) &= (x_1x_2, y_1y_2)(x_3, y_3) \\
&= \Big((x_1x_2)x_3, (y_1y_2)y_3\Big) \\
&= \Big(x_1(x_2x_3), y_1(y_2y_3)\Big) \\
&= (x_1, y_1)(x_2x_3, y_2y_3) \\
&= (x_1, y_1)\Big((x_2, y_2)(x_3, y_3)\Big),
\end{aligned}$$

   so multiplication in $G_1 \times G_2$ is associative. The identity is $(e, f)$ where $e$ is the identity in $G_1$ and $f$ is identity in $G_2$ since $(e, f)(x, y) = (ex, fy) = (x, y)$ and $(x, y)(e, f) =$

$(xe, yf) = (x, y)$ for any $(x, y) \in G_1 \times G_2$. If $(x, y) \in G_1 \times G_2$, then

$$(x^{-1}, y^{-1})(x, y) = (x^{-1}x, y^{-1}y) = (e, f) = (xx^{-1}, yy^{-1}) = (x, y)(x^{-1}, y^{-1}),$$

so $(x, y)^{-1} = (x^{-1}, y^{-1})$. Hence we conclude that $G_1 \times G_2$ is a group under $*$.

Now define $\varphi : G_1 \times G_2 \to G_2 \times G_1$ via $\varphi(x, y) = (y, x)$. This is a homomorphism, since

$$\begin{aligned}\varphi\Big((x_1, y_1)(x_2, y_2)\Big) &= \varphi\Big((x_1x_2, y_1y_2)\Big) \\ &= (y_1y_2, x_1x_2) \\ &= (y_1, x_1)(y_2, x_2) \\ &= \varphi\Big((x_1, y_1)\Big)\varphi\Big((x_2, y_2)\Big)\end{aligned}$$

for all $x_1, x_2 \in G_1$ and $y_1, y_2 \in G_2$. Each $(y, x) \in G_2 \times G_1$ is the image of $(x, y)$ under $\varphi$, so $\varphi$ is surjective. Also if $(x, y) \in \mathrm{Ker}(\varphi)$, then $\varphi(x, y) = (y, x) = (f, e)$, so $(x, y) = (e, f)$ is the identity element of $G_1 \times G_2$, and hence $\mathrm{Ker}(\varphi) = \{(e, f)\}$. Therefore $\varphi$ is injective by question 3. We conclude that $\varphi$ is an isomorphism and hence $G_1 \times G_2 \cong G_2 \times G_1$.

6. Let $g, h \in G$. We need to prove that $\psi(gh) = \sigma_{gh}$ is equal to $\psi(g) \circ \psi(h) = \sigma_g \circ \sigma_h$. If $x \in G$ then $\sigma_{gh}(x) = (gh)x(gh)^{-1}$ and

$$(\sigma_g \circ \sigma_h)(x) = \sigma_g(hxh^{-1}) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1}.$$

Hence we conclude that $\psi(gh) = \sigma_{gh} = \sigma_g \circ \sigma_h = \psi(g) \circ \psi(h)$, and $\psi$ is a homomorphism.

Now let $g \in \mathrm{Ker}(\psi)$. We have $\psi(g) = \sigma_g = i_G$, the identity map on $G$. Hence for every $x \in G$ we have $\sigma_g(x) = gxg^{-1} = x$, which implies $gx = xg$. Therefore $g \in Z(G)$ and hence $\mathrm{Ker}(\psi) \subset Z(G)$. Conversely, let $g \in Z(G)$. We have $gx = xg$ for all $x \in G$. Hence $gxg^{-1} = \sigma_g(x) = x = i_G(x)$ for every $x \in X$. Therefore $g \in \mathrm{Ker}(\psi)$. This shows that $Z(G) \subset \mathrm{Ker}(\psi)$ and hence $\mathrm{Ker}(\psi) = Z(G)$.

7. Let $n \in \theta(N)$ and $g \in G$. We need to show that $g^{-1}ng \in \theta(N)$. For this, set $n' := \theta^{-1}(n)$ and $g' := \theta^{-1}(g)$, and note that $g'^{-1}n'g' \in N$ (since $n' \in N$ and $N \trianglelefteq G$). It follows that

$$g^{-1}ng = \theta(g')^{-1}\theta(n')\theta(g') = \theta(g'^{-1}n'g') \in \theta(N).$$

8. Pick a point $v_1 \in \mathbb{R}^2$ fixed by $s$ (for example $v_1 := (0, 1)$). Also set $v_2 := r(v_1)$ and $v_3 := r(v_2)$. The idea is that $V := \{v_1, v_2, v_3\}$ is the set of vertices of a triangle in the plane. Since $r$ has order 3, $r(v_3) = v_1$ and hence $r(V) = V$. Moreover

$$s(v_2) = s(r(v_1)) = (sr)(v_1) = (r^{-1}s)(v_1) = r^{-1}(v_1) = v_3$$

and similarly $s(v_3) = v_2$. It follows that $s(V) = V$, and therefore $g(V) = V$ for all $g \in D_6$.

So if $g \in D_6$, we can define its restriction $r(g) : V \to V$ (which just sends $v \mapsto g(v)$). Note that $r(gh) = r(g)r(h)$ for all $g, h \in D_6$; indeed

$$r(gh)(v) = (gh)(v) = g(h(v)) = g(r(h)(v)) = r(g)(r(h)(v)) = (r(g)r(h))(v)$$

for all $v \in V$. In particular $r(g^{-1})r(g) = r(g^{-1}g) = r(e) = e$ and similarly $r(g)r(g^{-1}) = e$; in other words $r(g^{-1})$ is the inverse of $r(g)$. Therefore $r$ defines a function $D_6 \to A(V)$, which is a homomorphism by the above calculation.

To show that $r$ is an isomorphism, it suffices to prove injectivity, because $D_6$ and $A(V)$ are finite sets of the same size. If $g \in \text{Ker}(r)$ then the restriction of $g$ to $V$ is the identity, so $g$ fixes $v_1$ and $v_2$. You can check that these two vectors give a basis for $\mathbb{R}^2$. Since the elements of $D_6$ are linear transformations (because $r$ and $s$ are), it follows that $g$ fixes every vector in $\mathbb{R}^2$. This shows that $\text{Ker}(r) = \{e\}$, as required.

It remains to prove that $A(V) \cong S_3$. For this, define $f : \{1, 2, 3\} \to V$ by $f(i) = v_i$. I hope it is clear that $f$ is a bijection. Next, we can define $\varphi : S_3 \to A(V)$ by $\varphi(x) = f^{-1}xf$. If $x, y \in S_3$ then

$$\varphi(xy) = f^{-1}xyf = f^{-1}xff^{-1}xf = \varphi(x)\varphi(y),$$

so $\varphi$ is a homomorphism. It is bijective because it has an inverse given by $g \mapsto fgf^{-1}$. Therefore $\varphi$ is an isomorphism, so $D_6 \cong A(V) \cong S_3$.

For the challenge problem, let $G$ be a nonabelian group of order 6. By Lagrange's theorem, elements of $G$ can have orders 1, 2, 3 and 6. If $g \in G$ has order 6, then $\langle g \rangle$ is a subgroup of $G$ with order 6, so $\langle g \rangle = G$, contradicting the assumption that $G$ is nonabelian. Therefore $G$ only has elements of orders 1, 2 and 3. The set $\{g \in G \mid o(g) = 3\}$ can be partitioned into subsets of the form $\{g, g^{-1}\}$ (with $g \neq g^{-1}$) so $G$ has an even number of elements of order 3, i.e. either 0, 2, 4 or 6. It cannot have 6 because $o(e) = 1$, and it cannot have 0 by Problem 2 on Homework 2 (if $g^2 = e$ for all $g \in G$, then $G$ is abelian).

Next, let $g, h \in G$ have orders 2 and 3 respectively. Suppose for a contradiction that $gh = hg$. Since $C(g)$ contains $g$ and $h$, both 2 and 3 divide $|C(g)|$ by Lagrange's theorem. Therefore $C(g) = G$, and similarly $C(h) = G$. Given any $g' \in G$ of order 2, it follows that $g'h = hg'$, and the same argument shows that $C(g') = G$. Similarly $C(h') = G$ for any $h' \in G$ of order 3. Therefore every element of $G$ is central, which is impossible because $G$ is nonabelian. The upshot is that $gh \neq hg$, or equivalently $h^{-1}gh \neq g$. This shows that $G$ has at least two elements of order 2 (namely $g$ and $h^{-1}gh$), so it cannot have 4 of order 3. Therefore $G$ has 3 elements of order 2 and 2 of order 3.

Let $T := \{g \in G \mid o(g) = 2\}$. As above we can easily show that $A(T) \cong S_3$. Each $g \in G$ defines a function $\varphi(g) : T \to T$ by sending $t \mapsto gtg^{-1}$. If $g, h \in G$ then

$$\varphi(gh)(t) = ght(gh)^{-1} = ghth^{-1}g^{-1} = g\varphi(h)(t)g^{-1} = \varphi(g)(\varphi(h)(t)) = (\varphi(g)\varphi(h))(t)$$

for all $t \in T$, so $\varphi(gh) = \varphi(g)\varphi(h)$. It follows that $\varphi(g^{-1})$ is the inverse of $\varphi(g)$, and in partcular $\varphi$ defines a function $G \to A(T)$. The above calculation shows that $\varphi$ is a homomorphism. As above it remains to show that $\varphi$ is injective. For this, let $g \in \mathrm{Ker}(\varphi)$. Since $\varphi(g)$ is the identity function $T \to T$, $g$ commutes with every element of $T$. In other words $T \subseteq C(g)$, which implies that $|C(g)| \geq 4$ (since $e \in C(g)$ also). Therefore $g$ is central by Lagrange's theorem. This forces $g = e$, because the elements of order 2 do not commute with those of order 3, and vice versa.

9 & 10. We will tackle these at the same time, because if $\mathrm{Isom}(T) \cong S_4$ then $|\mathrm{Isom}(T)| = 24$. The $3 \times 3$ identity matrix obviously belongs to $\mathrm{Isom}(T)$. Moreover, if $B, C \in \mathrm{Isom}(T)$ then $B$ and $C$ give bijections $T \to T$, so $BC$ and $B^{-1}$ also give bijections $T \to T$, and hence $BC, B^{-1} \in \mathrm{Isom}(T)$. Thus $\mathrm{Isom}(T) \leq \mathrm{GL}_3(\mathbb{R})$, and in particular $\mathrm{Isom}(T)$ is a group.

Let $V = \{v_1, v_2, v_3, v_4\}$ be the set of vertices of $T$. The second paragraph of Problem 8 (with some minor adjustments) shows that the restriction map $r : \mathrm{Isom}(T) \to A(V)$ is a homomorphism. It is injective by another similar argument: any three vertices give a basis for $\mathbb{R}^3$, and the elements of $\mathrm{Isom}(T)$ are literally matrices this time. To check that any three vertices give a basis, it might be easiest to check the first three directly, then express all four in that basis. Since $v_1 + v_2 + v_3 + v_4 = 0$ you will get $\{e_1, e_2, e_3, (-1, -1, -1)\}$, where $e_i$ is the $i$th standard basis vector (the $i$th column of the $3 \times 3$ identity matrix). This set is a bit easier to deal with.

To prove that $r$ is onto, we have to do some work (because $|\mathrm{Isom}(T)|$ is unknown). For each $f \in A(V)$ let $M_f$ be the $3 \times 3$ matrix with columns $f(v_1)$, $f(v_2)$ and $f(v_3)$. Since any three vertices give a basis for $\mathbb{R}^3$, these matrices are all invertible. By definition $M_f e_i = f(v_i)$, and hence $M_f M_e^{-1} v_i = f(v_i)$, for each $i \in \{1, 2, 3\}$. It follows that

$$M_f M_e^{-1} v_4 = M_f M_e^{-1}(-v_1 - v_2 - v_3) = -f(v_1) - f(v_2) - f(v_3) = f(v_4)$$

(the last step follows from the formula $v_1 + v_2 + v_3 + v_4 = 0$ and the fact that $f$ is bijective). This shows that $r(M_f M_e^{-1}) = f$, if you are willing to accept that $M_f M_e^{-1} \in \mathrm{Isom}(T)$. To prove this, note that $T$ is the *convex hull* of $V$, which means it is the set of *convex* linear combinations of elements of $V$. A linear combination $\sum_{i=1}^4 a_i v_i$ is convex provided that the coefficients are nonnegative and add up to 1. So if $t \in T$ then $t = \sum_{i=1}^4 a_i v_i$ for some $a_i \geq 0$ with $\sum_{i=1}^4 a_i = 1$, and hence $M_f M_e^{-1} t = \sum_{i=1}^4 a_i M_f M_e^{-1} v_i = \sum_{i=1}^4 a_i f(v_i) \in T$.