Algebra II. Exercise 3.
Solutions.

1. a) If $|X| = n$, then $|\mathrm{Sym}(X)| = n!$, see for example Proposition 4.4 [Häsä–Rämö, p. 67].

b) If $|G| > |\mathrm{Sym}(X)|$, then the function $\varphi\colon G \to \mathrm{Sym}(X)$ defining the action, cannot be injective. Thus two different elements g, g' of G give the same permutation, that is, $gx = g'x$ for every $x \in X$.

If $gx = g'x$ for every $x \in X$, then $g^{-1}(gx) = g^{-1}(g'x)$, that is, $x = (g^{-1}g')x$ for every $x \in X$. Hence for the element $\bar{g} = g^{-1}g'$ we have $\bar{g}x = x$ for every $x \in X$; moreover $\bar{g} \neq e$, since $g \neq g'$.

Alternative solution: If $\varphi\colon G \to \mathrm{Sym}(X)$ is injective, then we have $|\mathrm{Im}(G)| = |G|$. Now $\mathrm{Im}(G)$ is a subgroup of $\mathrm{Sym}(X)$, and thus $|\mathrm{Im}(G)|$ divides $|\mathrm{Sym}(X)|$, that is, $|G|$ divides $|\mathrm{Sym}(X)|$. Hence if $|G|$ doesn't divide $|\mathrm{Sym}(X)|$, then φ cannot be injective.

2. Let X be a G-set, $Y \subset X$.

We prove that the stabilizer G_Y is a submonoid:

- $e_G \in G_Y$, since $e_G y = y \in Y$ for every $y \in Y$.
- If $g_1, g_2 \in G_Y$ and $y \in Y$, then $g_2 y = y'$ for some $y' \in Y$ and $g_1 y' \in Y$, and we obtain
$$(g_1 g_2)y = g_1(g_2 y) = g_1 y' \in Y$$
and thus $g_1 g_2 \in G_Y$.

The stabilizer is not always a subgroup: Choose $G = (\mathbb{Z}, +)$, $X = \mathbb{Z}$ and define the action by the formula $(n, x) \mapsto n + x$. Now the stabilizer of the subset $\mathbb{N}$ is $\{0, 1, 2, ...\}$, which is not a subgroup of $\mathbb{Z}$.

Next we prove that if Y is finite, then $G_Y \leq G$: Let $g \in G_Y, y \in Y$. From the above it follows by induction that
$$\{g^n y \mid n \in \mathbb{N}\} \subset Y.$$

Since Y is finite, there exist i, j, $i < j$, such that $g^i y = g^j y$. From this we obtain $g^{-1}y = g^{-i-1}g^i y = g^{-i-1}g^j y$, and thus $g^{-1}y = g^{j-i-1}y \in Y$, because

$j-i-1 \geq 0$. Thus $g^{-1} \in G_Y$. Earlier we proved that G_Y is a submonoid and now we proved $[g \in G_Y \Rightarrow g^{-1} \in G_Y]$, so G_Y is a subgroup.

The previous fact can also be proved as follows. Let $g \in G_Y$. Then acting by the element g gives a map $f_g\colon Y \to Y$, which is injective (since acting by g gives a bijection $X \to X$). Since Y is finite, an injective map is also surjective. Thus acting by the element g^{-1} also gives a map $Y \to Y$, that is $g^{-1} \in G_Y$.

Finally we prove that if G_Y is finite, then $G_Y \leq G$: Let $x \in G_Y$. Consider the powers $x^0, x^1, x^2, \ldots,$ of x, which are in G_Y, since G_Y is a submonoid. Since G_Y is finite, there exist $i, j,\ i < j$, such that $x^i = x^j$. Now $x^{j-i} = e_G$, and thus $x \cdot x^{j-i-1} = x^{j-i} = e_G$. Moreover $x^{j-i-1} \in G_Y$, because $j-i-1 \geq 0$. Thus $x^{-1} = x^{j-i-1} \in G_Y$.
Observe that the action of G was not used in the last proof, so actually we proved that a finite submonoid of a group is always a subgroup.

3. As a product of cycles $\tau = (1\ 5\ 4\ 7)(2\ 3)(6) = (1\ 5\ 4\ 7)(2\ 3)$, as a product of transpositions $\tau = (1\ 5)(5\ 4)(4\ 7)(2\ 3)$. Since in the representation of $\tau \in S_7$ as a product of disjoint cycles there are 3 cycles (when counting also the 1-cycles), we have that $\operatorname{sgn}(\tau) = (-1)^{7-3} = 1$. This can also be seen from the fact that when τ is represented as a product of transpositions, there are an even number of transpositions.
If $\sigma = (1\ 3)(5\ 2\ 6)$, then using for example Proposition 3.6 we obtain directly that $\sigma\tau\sigma^{-1} = (3\ 2\ 4\ 7)(6\ 1)$.

4. a) A direct calculation shows that the permutations $\alpha = (ij)(kl)$ and $\beta = (ilk)(ijk)$ operate similarly on each element: $\alpha(i) = j = \beta(i)$, $\alpha(j) = i = \beta(j)$, $\alpha(k) = l = \beta(k)$ and $\alpha(l) = k = \beta(l)$. Thus they are the same permutation. Similarly we can check that $(ij)(ik) = (ikj)$.

b) Every 3-cycle is an even permutation in S_n, that is, belongs to A_n. Thus also the subgroup H generated by the 3-cycles is contained in A_n. To prove our claim, it is sufficient to show that $A_n \subset H$, that is, every even permutation can be represented as a product of 3-cycles. Let $\tau \in A_n$. Then τ can be represented as a product of transpositions, and the number of transpositions is even, since τ is an even permutation:

$$\tau = \sigma_1 \sigma_2 \cdots \sigma_{2n-1}\sigma_{2n},$$

for some $n \geq 0$. By item a) every product $\tau_i = \sigma_{2i-1}\sigma_{2i}$ can be presented as a 3-cycle or a product of two 3-cycles, $i = 1, ..., n$. From this it follows that also $\tau = \tau_1 \cdots \tau_n$ can be represented as a product of 3-cycles.

(Observe that if a product of two transpositions consists of three or four different numbers, it can be written in a form considered in item a). If it contains only two different numbers, it is of the form $(ij)(ij)$, which gives the identity. It cannot consist of only one number.)

5. a) Suppose first that H is a normal subgroup of G. Let $x, y \in G$ be elements, for which $xH = yH$. By normality we have that $xH = Hx$ and $yH = Hy$, so $Hx = Hy$ and we have

$$x^{-1}H = \{x^{-1}h \mid h \in H\} = \{(h^{-1}x)^{-1} \mid h \in H\} = \{(hx)^{-1} \mid h \in H\}$$

$$= \{(hy)^{-1} \mid h \in H\} = ... = y^{-1}H.$$

In the third step we used the fact that $H \leq G$ and in the fourth step the fact that $Hx = Hy$. This proves the implication in the other direction.

This proof can also be written as follows: Suppose H is a normal subgroup. Then

$$xH = yH \Rightarrow y^{-1}xH = H \Rightarrow Hy^{-1}x = H \Rightarrow Hy^{-1} = Hx^{-1} \Rightarrow y^{-1}H = x^{-1}H.$$

To prove the implication in the other direction, suppose that $x \in G, h \in H$. Then $xh^{-1}H = xH$, and by the assumption we have $hx^{-1}H = x^{-1}H$. From this it follows that $hx^{-1} \in x^{-1}H$ and thus $xhx^{-1} \in H$. This holds for every $h \in H$, so

$$xHx^{-1} \subset H \text{ for every } x \in G.$$

This proves that H is a normal subgroup of G.

b) By the assumption $[G : H] = 2$ there are exactly two left cosets, namely H itself and xH for some $x \notin H$. From this it follows that the condition $xH = yH$ can be stated in the form "$x \in H$, if and only if $y \in H$". Since H contains all inverses of its' elements, it follows that "$x^{-1} \in H$, if and only if $y^{-1} \in H$". On the other hand this means that $x^{-1}H = y^{-1}H$, and hence by item a) we have that H is normal.

An alternative solution to b): Suppose that $h \in H$ and $g \in G$. Let $a \notin H$, so aH is a different coset than H and hence $G = H \cup aH$. If $g \in H$, then clearly $ghg^{-1} \in H$. Suppose then that $g \notin H$. Now $g \in aH$ and there exists

$k \in H$, for which $g = ak$. If we would have $ghg^{-1} = akhk^{-1}a^{-1} \notin H$, then we would have $akhk^{-1}a^{-1} = am$ for some $m \in H$. Then $a = m^{-1}khk^{-1}$ is an element of the subgroup H, which is a contradiction. Thus $ghg^{-1} \in H$ also in this case. This proves that H is a normal subgroup.

6. Suppose that G is a group, $g \in G$. Define

$$f_g\colon G \to G$$

by the formula

$$x \mapsto gx;$$

then we have $f_e = \mathrm{id}_G$ and moreover $f_g \circ f_h = f_{gh}$ for every $g, h \in G$, thus the conditions of an action hold. Hence every f_g is bijective and we can define

$$F\colon G \to \ \mathrm{Sym}(G)$$

$$g \mapsto f_g.$$

By the formula $f_g \circ f_h = f_{gh}$ we have that F is a group homomorphism $G \to (\mathrm{Sym}(G), \circ)$. We prove that F is injective: It is sufficient to prove that $\mathrm{Ker}(F) = \{e\}$. If $g \in G$ is such that $F(g) = f_g = \mathrm{id}_G$, then $f_g(e) = \mathrm{id}_G(e) = e$ and on the other hand $f_g(e) = ge = g$. Thus $g = e$, and we have that $\mathrm{Ker}(F) = \{e\}$.

Thus F defines an isomorphism $G \to \mathrm{Im}(F) \subset \mathrm{Sym}(G)$, that is, G is isomorphic with the subgroup $\mathrm{Im}(F)$ of the group $\mathrm{Sym}(G)$.