Exercises 3, 8, 20, 23, 25, pp. 40-41;

3. ($\Rightarrow$): If H is abelian, then for any $a, b \in G$, $\varphi(ab) = \varphi(a)\varphi(b) = \varphi(b)\varphi(a) = \varphi(ba)$, where we use all our hypotheses. But φ is injective, so $ab = ba$. Hence G is abelian.

   ($\Leftarrow$): If G is abelian, then do the same argument with φ^{-1}. For any $a, b \in H$, $\varphi^{-1}(ab) = \varphi^{-1}(a)\varphi^{-1}(b) = \varphi^{-1}(b)\varphi^{-1}(a) = \varphi^{-1}(ba)$. Now φ^{-1} is injective, so G is abelian.

8. The orders of S_n and S_m are $n!$ and $m!$, respectively. Since sizes are non-equal so there cannot exist a bijection between S_n and S_m.

20. We prove the group axioms for $\mathrm{Aut}(G)$.

   (a) *Identity*: Let $\mathrm{id}_G : G \to G$ be the identity. Clearly for any $\varphi \in \mathrm{Aut}(G)$, $\varphi \circ \mathrm{id}_G = \mathrm{id}_G \circ \varphi = \varphi$. Hence id_G is the identity.

   (b) *Associativity*: Note that function composition is associative, so multiplication in $\mathrm{Aut}(G)$ is by definition associative.

   (c) *Closure*: We need to prove that for any $\varphi, \phi \in \mathrm{Aut}(G)$, $\varphi \circ \phi \in \mathrm{Aut}(G)$. Indeed, if φ and ϕ are isomorphisms, then for any $g, h \in G$, $\varphi(\phi(gh)) = \varphi(\phi(g)\phi(b)) = \varphi(\phi(g))\varphi(\phi(h))$. Hence $\varphi \circ \phi$ is a homomorphism. Furthermore, the composition of two bijections is a bijection, so $\varphi \circ \phi$ is a isomorphism as well.

   (d) *Inverses*: If $\varphi \in \mathrm{Aut}(G)$, then the function inverse $\varphi^{-1} G \to G$ is also the inverse of φ in $\mathrm{Aut}(G)$.

23. To show that every element g can be written as $x^{-1}\sigma(x)$, it is equivalent to prove that the map $x \mapsto x^{-1}\sigma(x)$ is surjective. Since G is finite, this is equivalent to showing that $x \mapsto x^{-1}\sigma(x)$ is injective via a cardinality argument.

    Let $x, y \in G$ such that $x^{-1}\sigma(x) = y^{-1}\sigma(y)$. Then rearrange to get $\sigma(x)\sigma(y)^{-1} = \sigma(xy^{-1}) = xy^{-1}$. The the fact that *sigma* only fixes the dientity means that $xy^{-1} = 1 \Rightarrow x = y$. Hence $x \mapsto x^{-1}\sigma(x)$ is injective, we can conclude from above considerations that it is bijective.

    So, for any $g \in G$ we an find $x \in G$ such that $g = x^{-1}\sigma(x)$. Use the hint from the text and apply σ to both sides to get $\sigma(g) = \sigma(x^{-1})\sigma^2(x) = \sigma(x)^{-1}x$. Aha! We can see that, in fact, $\sigma(g) \cdot g = \sigma(x)^{-1}x \cdot x^{-1}\sigma(x) = 1$, so $g = \sigma(g^{-1})$. Then we have, for any $g, h \in G$,

    $$gh = \sigma(g^{-1})\sigma(h^{-1}) = \sigma(g^{-1}h^{-1}) = \sigma((hg)^{-1}) = hg,$$

    which proves that G is abelian!

25. (a) Geometrically, you can draw it out and see that if we apply $\begin{pmatrix} x \\ y \end{pmatrix}$ to the matrix, we get $\begin{pmatrix} x\cos\theta - y\sin\theta \\ x\sin\theta + y\cos\theta \end{pmatrix}$, which rotates the input by θ radians counterclockwise.

Exercises 4, 5, 6, 20, 21, pp. 44-45.

4. (a) We proceed by using the subgroup formula. Let H be the kernel of the action of G on A. Suppose $x, y \in H$, i.e. both x and y fix all elements of A. Then for any $a \in A$, we have $(xy^{-1}) \cdot a) = x \cdot (y^{-1} \cdot a)$. We know that $y \cdot a = a$, so $a = y^{-1} \cdot a$. Hence we can simplify $(xy^{-1}) \cdot a = a$ and conclude that $xy^{-1} \in H$. Hence H is a subgroup.

   (b) Let $G_a = \{g \in G : ga = a\}$. We use the subgroup formula again. Suppose $x, y \in G_a$. Again, $(xy^{-1}) \cdot a = x \cdot (y^{-1} \cdot a) = x \cdot a = a$. Hence $xy^{-1} \in G_a$ and we have a subgroup.

5. The kernel K of the group action of G on A is defined as $\{g \in G : \forall a \in A, ga = a\}$. If $g \in K$, then the permutation σ_g associated with g is the identity permutation. But we have $\varphi : G \to S_A$ defined by $\varphi(g) = \sigma_g$, so $\sigma_g = 1 \Rightarrow g \in \ker\varphi$. Hence $K \subseteq \ker\varphi$.

   For the other inclusion, consider $g \in \ker\varphi$. Then σ_g is the identity permutation, so clearly $ga = a$ for all $a \in A$. Then $g \in K$. Hence the two subgroups K and $\ker\varphi$ are equal.

6. For a faithful action of G on A, the corresponding permutation representation is injective. Hence $\ker\varphi$ is the trivial subgroup. By exercise 5, the kernel of the action is therefore also trivial.

20. Imagine the group of such rigid motions G acting on the vertices of the tetrahedron. Then we have an action from G on {four vertices}. This is equivalent to a homomorphism $\varphi : G \to S_4$. Furthermore, the only action that fixes all the vertices is clearly the trivial action. Hence the action is faithful, and G embbeds into S_4, i.e. G is isomorphic to its image (which is some subgroup) in S_4 under φ.

21. Let the rigid motions of the cube G act on the four pairs of opposite vertices that make up the cube. This is a valid action because opposite vertices remain opposite after rigid motions. The associated permutation representation is a map $\varphi : G \to S_4$. Furthermore, the only action that does not permute any vertices is the identity action. Then G acts faithfully; hence φ is injective.

    Now we prove that φ is surjective. Let σ be some permutation of opposite pairs of vertices. First pick some set of vertices and map them to the desired image. Then there are 3 choices in how to rotate the other 3 pairs to fit σ. This give 8 choices to pick the first pair and (4 pair locations times 2 orientations each) and 3 more choices. In total, that is 24 choices, meaning φ must also be surjective. Hence φ is bijective and is a group isomorphism.

Exercises 8, 10, 15 ,17, pp. 48-49.

8. ($\Rightarrow$): If $H \subseteq K$ or $K \subseteq H$, then either $H \cup K = K$ or $H \cup K = H$. In both cases $H \cup K$ is a subgroup of G.

   ($\Leftarrow$): If $H \cup K$ is a subgroup of G, then suppose for the sake of contradiction assume that $H < H \cup K$ and $K < H \cup K$, so there is some $h \in H$ such that $h \notin K$ and some $k \in K$ such that $k \notin H$. Consider the product $hk \in H \cup K$. Then $hk = h' \in H$ or $hk = k' \in K$. In the first case, we have $k = h^{-1}h' \in H$ which gives contradiction. In the second case, we have $h = k^{-1}k' \in K$ which also gives contradiction. Therefore the proof is complete.

10. (a) We proceed with the subgroup formula. Let $x, y \in H \cap K$. Then $x \in H$ and $y^{-1} \in H$, so $xy^{-1} \in H$. Similarly, $x \in K$ and $y^{-1} \in K$, so $xy^{-1} \in K$. Hence $xy^{-1} \in H \cap K$.

    (b) Again we use the subgroup formula. Let $\mathcal{I}$ be some index set. Let $x, y \in \bigcup_{i \in \mathcal{I}} H_i$ for subgroups $H_i \leq G$ over all $i \in \mathcal{I}$. Then for each i, we have $x, y^{-1} \in H_i$ by definition of the intersection. Hence defintionally we have $xy^{-1} \in \bigcup_{i \in \mathcal{I}} H_i$, as desired.

15. We use the subgroup formula. Let $x, y \in \bigcup_{i=1}^{\infty} H_i$. Then there exist some i, j such that $x \in H_i$ and $y \in H_j$. Without loss of generality assume that $i \leq j$ (if it's not then just swap the variables around). Then $H_i \leq H_j$, so $x \in H_j$ and $xy^{-1} \in H_j \subseteq \bigcup_{i=0}^{\infty} H_i$, and the subgroup formula is satisfied.

17. Set $G = \{(a_{ij}) \in GL_n(F) : \forall i > j, a_{ij} = 0\}$. First, we have to show that $G \subseteq GL_n(F)$. Indeed, note that all the elements of G are in reduced row echelon form, so their determinants are simply that product of the diagonals, which is clearly 1. Hence all elements in G have inverses, i.e. $G \subseteq GL_n(F)$.

    We proceed by proving the group axioms. Clearly $I_n \in G$ is the identity.

    Next, we prove that G is closed under inverses. Suppose $A, B \in G$ are upper triangular. Then for $1 \leq i, j \leq n$, consider $AB_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$. If $i > j$, then $k > i \Rightarrow k > j$ and $j > k \Rightarrow i > k$, so are the terms have either $a_{ik} = 0$ or $a_{kj} = 0$. Hence $(AB)_{ij} = 0$. Of course when $i = j$, we have only the term $a_{ik}b_{kj} = 1$ when $k = i = j$, so $(AB)_{ii} = 1$. Hence G is closed under multiplication.

    Finally, we need to show that G has inverses. Let $A \in G$ and $B \in GL_n(F)$ such that $AB = I_n$. Note that if $i = n$, then we have $b_{kj} = 0$. Extending this by doing induction on i shows that $b_{kj} = 0$ for all $k > j$. Hence $B \in G$, and G has inverses.