Unit 2: Subgroups

2.1 The definition and some examples. Let \((G, \cdot)\) denote an arbitrary group. A **subgroup** of \(G\) is a nonempty subset \(H\) of the set \(G\) that is a group in its own right when the operation “\(\cdot\)” from \(G\) is restricted to the set \(H\). That is, a nonempty subset \(H\) of \(G\) is a subgroup of \(G\) provided that \((H, \cdot)\) is a group also.

In order for this to happen, it must be the case that “\(\cdot\)” is a binary operation on \(H\) as well as being a binary operation on \(G\). Recall that when we say that “\(\cdot\)” is a binary operation on \(G\), we mean that “\(\cdot\)” returns an element of \(G\) whenever one uses “\(\cdot\)” to combine two elements of \(G\). If “\(\cdot\)” is also going to be an operation on \(H\), this means that if the two input elements \(a\) and \(b\) come for the subset \(H\), then the output element \(a \cdot b\) is also in \(H\). When this happens, we say that \(H\) is closed under “\(\cdot\)”.

**Example 1:** The set \(\mathbb{Q}\) of all rational numbers is a subset of \(\mathbb{R}\), the set of all real numbers. One can check that \((\mathbb{Q}, +)\) is a subgroup of \((\mathbb{R}, +)\).

**Example 2:** In the group \((\mathbb{R}^*, \cdot)\) of nonzero real numbers with multiplication as the operation, the set \(\mathbb{Q}^*\) of all nonzero rational numbers is a subgroup.

**Example 3:** The set \(\mathbb{Z}\) of all integers is a subset of \(\mathbb{Q}\), the set of all rational numbers. One can check that \((\mathbb{Z}, +)\) is a subgroup of \((\mathbb{Q}, +)\).

**Example 4:** The set \(A_n\) of all even permutations in \(S_n\) forms a subgroup of \(S_n\).

**Example 5:** Let us denote by \(\mathcal{F}\) the set of all functions from the real numbers to the real numbers. This set can be made into a group by taking the usual addition of functions as the operation. (For two functions \(f\) and \(g\) in \(\mathcal{F}\), the sum \(f + g\) of these functions is the function defined at all \(x\) in \(\mathbb{R}\) by the formula \((f+g)(x) = f(x) + g(x)\).) Now let \(\mathcal{D}\) be the subset of \(\mathcal{F}\) consisting of those functions that are differentiable everywhere, that is, which have a derivative at every \(x\) in \(\mathbb{R}\). This subset \(\mathcal{D}\) is a subgroup of \(\mathcal{F}\). The key insight is that when you add two functions which are differentiable, you get back a function which is differentiable. We remember this fact via the rule “the derivative of a sum is the sum of the derivatives.”

**Example 6:** Let us denote by \(\mathcal{F}^*\) the set of all functions from the real numbers to the real numbers which do not take on the value zero anywhere. This set can be made into a group by taking the usual multiplication of functions as the operation. (For two functions \(f\) and \(g\) in \(\mathcal{F}^*\), the product \(f \cdot g\) of these functions is the function defined at all \(x\) in \(\mathbb{R}\) by the formula \((f \cdot g)(x) = f(x) \cdot g(x)\).) Now let \(\mathcal{E}^*\) be the
subset of $\mathcal{F}^*$ consisting of those functions that are continuous everywhere, that is, which satisfy the condition that \( \lim_{x \to a} f(x) = f(a) \) at every \( a \) in \( \mathbb{R} \). This subset \( \mathcal{C}^* \) is a subgroup of \( \mathcal{F}^* \). The key insight is that you get a continuous function back when you multiply two continuous functions together, a fact which follows from the definition of continuity and the rule “the limit of a product is the product of the limits.

These are just a few examples of subgroups. There are many more that are of interest. One of the major objectives of group theory is to identify the subgroups of a given group and to understand how these subgroups relate to the “parent” group that contains them and to each other.

There is a standard characterization of what it takes for a subset of a group to be a subgroup. We will state and prove it now.

**Theorem 2.1:** Let \((G, \cdot)\) be any group, and let \(H\) be any subset of \(G\). This subset \(H\) is a subgroup of \(G\) provided that these three conditions hold:

(a) \(H\) is nonempty.

(b) \(H\) is closed under the operation “\(\cdot\)” of \(G\). That is, \(a \cdot b\) is back in \(H\) whenever \(a\) and \(b\) are from \(H\).

(c) \(H\) is closed under the taking of inverses. That is, \(a^{-1}\) is back in \(H\) whenever \(a\) is in \(H\).

**Proof:** To show that \(H\) is a subgroup of \(G\), we need to verify that \((H, \cdot)\) is a group, where “\(\cdot\)” is the operation that \(H\) inherits from \(G\). First of all, we need to have \(H\) be a nonempty subset of \(G\), but this is something we are assuming to be true as set forth in (a). Second, we need to check that the operation “\(\cdot\)” of \(G\) works as an operation on \(H\) also in that it always returns an element of \(H\) whenever the two elements being combined come from \(H\). This is what our assumption (b) assures us.

Having verified these preliminary necessary conditions, we now consider whether the group axioms are satisfied by the operation “\(\cdot\)” on \(H\). The associativity axiom holding on \(H\) follows automatically from the fact that it holds on the larger set \(G\). Thus, we see that we have the associativity axiom holding for \((H, \cdot)\).

Next let us consider whether or not \(H\) contains an identity element. The possibility might be that there is an element of \(H\) that acts as an identity for the elements of \(H\), but that this element is a different one from
the identity of $G$. However this never what happens. It will always be the case that the identity element $e_G$ of $G$ has to be an element of $H$, and thus it serves as the identity element for this smaller set.

To see why this claim is true if our three conditions (a), (b), and (c) are true, we cite (a) which says that $H$ is nonempty, and let $d$ denote an arbitrary element of $H$. Now by (c), since $d$ is in $H$, its inverse, $d^{-1}$, is also in $H$. Now that we have established that $d$ and $d^{-1}$ are both elements of $H$, we may cite (b) to say that their product $d \cdot d^{-1}$ is also in $H$. However $d \cdot d^{-1}$ is $e_G$, so we have established that $e_G$ is in $H$. Since $e_G$ acts as an indentity element for all elements of $G$, it certainly does so for the elements of the subset $H$ of $G$. It thus is an identity element for $H$, so $(H, \cdot)$ satisfies the identity axiom.

Finally, let us consider whether $(H, \cdot)$ satisfies the inverse axiom. To do so, let us consider any element $a$ of $H$. We need to establish that $a$ has an inverse element in $H$. Since $a$ is an element of the larger group $G$, $a$ has an inverse in $G$ that we denote by $a^{-1}$. This means that $a \cdot a^{-1} = e_G$ and $a^{-1} \cdot a = e_G$.

Now by our assumption (c), this inverse $a^{-1}$ is also an element of $H$ since $a$ is from $H$. Also we just showed that $e_G$ is in $H$ and is the identity element for $H$. Thus, the element of $G$ that is the inverse in $G$ of $a$ is also the inverse of $a$ in $H$. This shows that $H$ satisfies the inverse axiom.

Now that we have checked that $(H, \cdot)$ satisfies all three of the group axioms, we have shown that $(H, \cdot)$ is a group, and thus $H$ is a subgroup of $G$.

We comment that the converse of Theorem 2.1 is also true. That is, if $H$ is a subgroup of a group $G$, then the conditions (a), (b), and (c) must be satisfied. We will leave the verification of this as an exercise.

2.2 Checking whether subsets are subgroups. Now that we have established Theorem 2.1, it will provide our standard method for checking to see if a given subset $H$ of a group $G$ is a subgroup. To show that $H$ is a subgroup, we will simply verify that $H$ satisfies the three conditions. To show that a set $H$ is not a subgroup, we will show that it fails to satisfy at least one of these conditions. Let us illustrate this with a few of the examples from the last section, as well as some few new examples of subsets which are not subgroups.

Example 7: The set $A_n$ of all even permutations in $S_n$ forms a subgroup of $S_n$, as claimed in Example 4. To see this, we note that since $\varepsilon = (1, 2)(1,2)$, the identity permutation $\varepsilon$ is expressible using an even number of transpositions and thus is even. This means that $A_n$ is not empty, so (a) is true.
To verify (b), let us take any two elements $a$ and $b$ in $A_n$. We need to verify that $\alpha \circ \beta$ is back in $A_n$, which means that we need to verify that $\alpha \circ \beta$ is even. Now since $\alpha$ and $\beta$ are in $A_n$, they are both even. This means that we can express $\alpha$ using an even number, say $k_1$, transpositions, and similarly, we can express $\beta$ using $k_2$ transpositions where $k_2$ is also even. We can get an expression for $\alpha \circ \beta$ in terms of transpositions by stringing together the $k_1$ that we use for $\alpha$ with the $k_2$ we use for $\beta$. This gives us an expression for $\alpha \circ \beta$ that uses $k_1 + k_2$ transpositions. Since $k_1$ and $k_2$ are both even, so is their sum, $k_1 + k_2$. This is sufficient to allow us to conclude that $\alpha \circ \beta$ is even and thus is back in $A_n$.

This verifies (b), the closure of $A_n$ under the operation.

Finally, let us verify (c), the closure of $A_n$ under inversion. To do so, let us take any element $\alpha$ in $A_n$. We need to show that $\alpha^{-1}$ is also in $A_n$. To do this, we need to show that $\alpha^{-1}$ is even, working of course from the assumption that $\alpha$ is even since we are assuming that $\alpha$ is in $A_n$. We see that this claim about $\alpha^{-1}$ is true if we recall that whatever expression we have for $\alpha$ in terms of transpositions, we get an expression for $\alpha^{-1}$ in terms of transpositions if we take the same ones and write them in the reverse order. Since we have an even expression of this form for $\alpha$, we get an even expression for $\alpha^{-1}$. Thus, we have shown that $\alpha^{-1}$ is in $A_n$ whenever $\alpha$ is, which shows that (c) is true.

Since we have verified all three of the conditions of Theorem 2.1, we have shown that $A_n$ is a subgroup of $S_n$.

Example 8: Let us verify the details of Example 6. That is, we will show that $E^*$ is a subgroup of $S^*$. We see that the identity function of $F^*$, which is the constant function $I$ which maps every nonzero $x$ in $R$ to 1, is an element of $E^*$, meaning that $E^*$ is not empty. To see why this is true, we need to convince ourselves that $I$ is a continuous function. We see that for every $a$ in the real numbers, $\lim_{x \to a} I(x) = \lim_{x \to a} 1 = I(a)$. This shows that $I$ is continuous everywhere, so $I$ is in $E^*$ and thus $E^*$ is not empty. (Note that $I$ never takes on the value 0, so thus it satisfies this condition for being in $E^*$.)

Next, let us take any two elements $f$ and $g$ in $E^*$. We need to verify that $f \cdot g$ is back in $E^*$. This means that we need to verify that $f \cdot g$ does not take on the value 0 and is continuous everywhere. The fact that $f \cdot g$ never takes on the value 0 follows from the fact that $f$ and $g$ separately never take on the value 0. This means that for every $a$ in $R$, $f(a) \neq 0$ and $g(a) \neq 0$. Since the product of two nonzero real numbers is always nonzero, we have that $f(a) \cdot g(a) \neq 0$. But by the definition for the multiplication of
functions, \( f \cdot g(a) = f(a) \cdot g(a) \), so we have that \( f \cdot g(a) \neq 0 \) for every real number \( a \). The other thing to be checked is that this product function \( f \cdot g \) is continuous at every real number \( a \). This follows from the string of equations \( \lim_{x \to a} f \cdot g(x) = \lim_{x \to a} f(x) \cdot g(x) = f(a) \cdot \lim_{x \to a} g(x) = f(a) \cdot g(a) = f \cdot g(a) \). (The successive equalities are justified by the definition of the product of two functions, the “limit of a product is the product of the limits” principle regarding limits, the assumption that both \( f \) and \( g \) are continuous at any \( a \) in the real numbers, and finally the definition of the product of two functions again.) We have now showed that \( f \cdot g \) satisfies the conditions to be in \( E^* \), and so we have verified condition (b) of the theorem.

Finally, let us verify (c) by showing that the inverse of \( f \) is back in \( E^* \) whenever \( f \) is in \( E^* \). For the operation of multiplication of functions, the inverse of a function \( f \) is called the reciprocal function of \( f \) and is denoted by \( 1/f \). It is defined by the rule \( (1/f)(x) = 1/f(x) \) for all \( x \). (We denote it in this way to distinguish from the other concept of inverse of a function, which is with respect to composition of functions. We reserve the superscript -1 notation \( f^{-1} \) for the inverse in this composition sense.)

To verify (c), let us take any \( f \) in \( E^* \). We will show that \( 1/f \) is also in \( E^* \). The first thing to observe is that \( (1/f)(x) \neq 0 \) for all real numbers \( x \). This is so because, since \( f \) is in \( E^* \), \( f(x) \neq 0 \) for all \( x \), which means that \( 1/f(x) \neq 0 \) for all \( x \). (In fact, we need \( f(x) \) to be nonzero in order that \( 1/f(x) \) be defined.)

Since we have \( (1/f)(x) = 1/f(x) \neq 0 \) for all \( x \) in \( \mathbb{R} \), we have the first condition for \( 1/f \) to be in \( E^* \). Let us now consider the other condition, namely that \( 1/f \) is continuous everywhere. We see that this string of equalities is true: \( \lim_{x \to a} (1/f)(x) = \lim_{x \to a} (1/f(x)) = \lim_{x \to a} 1/\lim_{x \to a} f(x) = 1/f(a) = (1/f)(a) \). (The successive equalities are justified by the definition of the reciprocal of a function, the “limit of a quotient is the quotient of the limits provided the limit of the denominator is not zero” principle regarding limits, the assumption that \( f \) is continuous at any \( a \) in the real numbers and the principle that the limit of a constant is that constant, and finally the definition of the reciprocal of a function again.) Now that we have shown that \( 1/f \) is continuous, we have seen what we need to see to be sure that \( 1/f \) is in \( E^* \). Thus, (c) of Theorem 2.1 is true.

Having verified all three conditions of Theorem 2.1 for the set \( E^* \), we have shown that it is a subgroup of \( F^* \).

2.3 The smallest subgroup containing a subset and cyclic subgroups. While not every subset of a
group is a subgroup, every nonempty subset \( S \) of a group \( G \) generates a uniquely determined subgroup of \( G \). What we mean by this is that it is possible to take a nonempty set \( S \) and to show that there is a smallest subgroup of \( G \) that contains \( S \) as a subset. This will be called the subgroup generated by \( S \) and will be denoted by \( <S> \).

**Theorem 2.2:** If \( (G, \cdot) \) is any group and if \( S \) is any nonempty subset of \( G \), then there exists a subgroup \( H \) of \( G \) such that

(a) \( S \subseteq H \).

(b) If \( K \) is any subgroup of \( G \) such that \( S \subseteq K \), then \( H \subseteq K \).

**Proof:** For our nonempty set \( S \), let us denote by \( \mathcal{H} \) the set of all the subgroups of \( G \) that contain \( S \). We observe that there is indeed at least one subgroup of \( G \) that contains \( S \), namely \( G \) itself. (Note by Theorem 2.1, every group is a subgroup of itself.) We will define the subgroup \( H \) we claim to exist to be the intersection of all of the subgroups of \( G \) contained in \( \mathcal{H} \). Thus,

\[
H = \{ x \mid x \in G \text{ and } x \in K \text{ for every } K \in \mathcal{H} \}.
\]

This says that the elements of \( H \) are precisely those elements of \( G \) that are in every subgroup of \( G \) that contains \( S \).

We verify that \( H \) is a subgroup of \( G \) by showing that it satisfies the conditions of Theorem 2.1. In showing that \( H \) is nonempty to verify (a) of Theorem 2.1, we will kill two birds with one stone and show (a) of this theorem as well. That is, we will show that \( S \subseteq H \). To see this, let us take any element \( x \) in \( S \). Since \( x \) is in \( S \), it clearly is in every subgroup \( K \) of \( G \) that contains \( S \). This is the condition for being in \( H \), so \( x \in H \). Since every \( x \) of \( S \) is in \( H \), this assures that \( S \subseteq H \), which means that (a) of this theorem is true. Since \( S \) is nonempty by our hypotheses, we have a nonempty subset of \( H \), which assures that \( H \) is nonempty, which assures that (a) of Theorem 2.1 is true.

To verify (b) of Theorem 2.1, let us take any two elements \( a \) and \( b \) of \( H \). We need to show that \( a \cdot b \) is also in \( H \). To show this, we need to show that \( a \cdot b \) is in every subgroup of \( G \) that contains \( S \). To this end, let us take a particular subgroup \( K \) of \( G \) which contains \( S \). Since \( a \in H \), because of the way \( H \) is defined, we can say that \( a \in K \). Similarly, \( b \in K \). Since \( K \) is a subgroup of \( G \), it is closed for the operation, so \( a \cdot b \in K \). Since this observation holds for every subgroup \( K \) of \( G \) which contains \( S \), we have \( a \cdot b \) satisfying the condition it must satisfy to be in \( H \). Thus, we conclude that \( a \cdot b \in H \), so \( H \) is closed for the operation on \( G \), and (b) of Theorem 2.1 is verified.
To verify (c) of Theorem 2.1, let us take any element \( a \) in \( H \). We need to verify that \( a^{-1} \) is also in \( H \).

To see this, we begin by taking any subgroup \( K \) of \( G \) that contains \( S \) and observing that by the way \( H \) is defined, \( a \in K \). Since \( K \) is a subgroup, it is closed under the taking of inverses, so \( a^{-1} \in K \). Since this holds for every subgroup \( K \) of \( G \) which contains \( S \), it follows that \( a^{-1} \) is in every such subgroup. This assures that \( a^{-1} \) is in \( H \). Thus, (c) of Theorem 2.1 is verified for this subset \( H \).

Having verified all three of the conditions of Theorem 2.1 for our set \( H \), we have shown that it is a subgroup of \( G \). We showed earlier that \( S \subseteq H \), which is claim (a) of our current theorem, but it remains to show (b), namely that \( H \) is a subset of every subgroup of \( G \) that contains \( S \). This is not a problem because of the way that \( H \) is defined. Since \( H \) is the intersection of all of the subgroups \( K \) of \( G \) which contain \( S \) as a subset, it clearly is a subset of all of these subgroups \( K \). Our proof is complete.

**Definition 2.3:** For any nonempty subset \( S \) of a group \( G \), we call this smallest subgroup of \( G \) which contains \( S \) the **subgroup of \( G \) generated by \( S \)**. We will denote it by \(<S>\).

This proof of the existence of \(<S>\) for every nonempty subset \( S \) is perfectly valid, but does not shed very much light on what this subgroup generated by \( S \) looks like. To see this, we need to think about it “from the inside.” Since a subgroup must be closed under the group operation and the taking of inverses, if a subgroup is going to contain a certain set \( S \) as a subset, it will have to contain all possible products and inverses of elements of \( S \). Consider the set that you get by taking all possible products and inverses and products of inverses of elements of \( S \). That is, we are taking all elements that can be expressed in the form \( a_1 \cdot a_2 \cdot a_3 \cdot \cdots \cdot a_m \) where \( m \) is any positive integer and each of the \( a_i \)'s is an element of \( S \cup S^{-1} \) where \( S^{-1} \) denotes the set of all inverses of the elements of \( S \). Clearly if a subgroup is going to contain \( S \) as a subset, it has to contain all products of this form. One can show that the set of all products of this form satisfies the three conditions of Theorem 2.1, so will have to be a subgroup of \( G \). This is another way of getting at \(<S>\).

**Example 9:** Consider the group \((\mathbb{Z}, +)\) of integers with addition as the operation, and let \( S = \{2, 3\} \).

What is the smallest subgroup of \( \mathbb{Z} \) that contains the two numbers \( 2 \) and \( 3 \)? We can show that it has to be all of \( \mathbb{Z} \). We see this by considering all things we can get combining the numbers \( 2 \) and \( 3 \) and \(-2\) and \(-3\). Recall that the operation here is addition, so we would use additive notation rather than the multiplicative notation that we used above when we were thinking in general. Note that \( 1 = 3 + (-2) \), and \(-1 = 2 + (-3) \), so we get \( 1 \) and \(-1 \) contained in any additive subgroup of \( \mathbb{Z} \) which contains \( 2 \) and \( 3 \). This means that any subgroup of \( \mathbb{Z} \) containing \( 2 \) and \( 3 \) must also contain any repeated sums of \( 1 \) and
Clearly all integers can be expressed as repeated sums of 1 or -1, so any subgroup of \( \mathbb{Z} \) which contains 2 and 3, in particular the smallest subgroup containing these two numbers, must contain all of the integers. As a result, we conclude that the subgroup generated by 2 and 3 is all of \( \mathbb{Z} \).

**Notation:** We would denote the subgroup generated by the set \{2, 3\} by \( \langle\{2, 3\}\rangle \), but to simplify the notation when we list all the elements in a small set, we drop the braces and denote this subgroup by \( \langle2, 3\rangle \).

**Example 10:** The subgroup \( \langle6, 15\rangle \) of \((\mathbb{Z}, +)\) is the same as the subgroup \( \langle3\rangle \), namely the set of all integral multiples of 3. To see this, let us note that we can get 3 by repeatedly adding and subtracting 6 and 15. One way is \( 3 = 15 - 6 - 6 \). Thus, a subgroup of \( \mathbb{Z} \) that contains 6 and 15 also has to contain 3. Once we know this, we can observe that it must contain all repeated sums of 3’s and -3’s, which we can see leads to all integral multiples of 3.

Now one can show that this set of all integral multiples of 3 is exactly what \( \langle3\rangle \) contains. Thus, we may conclude that \( \langle3\rangle \subseteq \langle6, 15\rangle \). However, since both 6 and 15 are multiples of 3, when we combine 6 and 15, we can only get multiples of 3. This means that \( \langle6, 15\rangle \subseteq \langle3\rangle \). Since we have set containment both ways on these two sets, we conclude that they are in fact equal, i.e., \( \langle6, 15\rangle = \langle3\rangle \).

**Definition 2.4:** For any element \( a \) of a group \( G \), we will denote the subgroup of \( G \) generated by \( a \) by \( \langle a \rangle \). We will call this the cyclic subgroup of \( G \) generated by \( a \).

Cyclic subgroups are easier to describe “from the inside” than more general subgroups generated by subset of a group.

**Theorem 2.3:** For any group \((G, \cdot)\) and any element \( a \) of \( G \), \( \langle a \rangle = \{a^i \mid i \in \mathbb{Z}\} \). That is, in a multiplicatively denoted group, the cyclic subgroup of \( G \) generated by an element \( a \) consists of all the integral powers of \( a \).

**Proof:** Recall that we observed that you get the subgroup generated by a set \( S \) of elements by taking all of the elements you get by repeatedly combining elements of \( S \cup S^{-1} \). In this case, \( S \) contains only one element, and the result of repeatedly combining it and its inverse yields the integral powers of the element.

To show this a different way, clearly the set of all integral powers of \( a \) forms a subgroup. It is
nonempty since \( a = a' \in \{ a' \mid i \in \mathbb{Z} \} \). The rule \( a^m \cdot a^n = a^{m+n} \) shows that the product of two integral powers of \( a \) is again an integral power of \( a \), so the set is closed under the operation. The rule \( (a^m)^{-1} = a^{-n} \) shows that the inverse of an integral power of \( a \) is again an integral power of \( a \), so the set of all integral powers of \( a \) is closed under the taking of inverses.

Since the set \( \{ a' \mid i \in \mathbb{Z} \} \) is a subgroup of \( G \), and since any subgroup containing \( a \) is going to have to contain all of the integral powers of \( a \), it follows that this set is in fact the subgroup generated by \( a \). That is, \( \langle a \rangle = \{ a' \mid i \in \mathbb{Z} \} \).

Note that although there are infinitely many integers and thus infinitely many representations for integral powers of \( a \), this does not necessarily mean that \( \langle a \rangle \) is an infinite set. It often happens that you start getting repeating as you go to higher powers. For example, if we take the 5-cycle \( \alpha = (1,2,3,4,5) \) in \( S_n \) for some \( n \) with \( n \geq 5 \), we have \( \varepsilon = \alpha^0 = \alpha^5 = \alpha^{10} = \alpha^{15} = \ldots \) and \( \alpha = \alpha^1 = \alpha^6 = \alpha^{11} \ldots \), etc. We see that we are cycling through the powers of \( \alpha \), which explains why this subgroup \( \langle \alpha \rangle \) is called a cyclic group. Note that in this case, the powers \( \alpha^0 \) through \( \alpha^4 \) of \( \alpha \) are all distinct from each other, and that each of the remaining powers equals one of these. That is, there are five distinct powers of \( \alpha \).

**Definition 2.5:** Let \((G, \cdot)\) be an arbitrary multiplicative group and let \( a \) be any element of \( G \). The order of \( a \) is the least positive integer \( k \) such that \( a^k = e \), where \( e \) denotes the identity element of \( G \). When \( k \) is the order of \( a \), we will write this as \( o(a) = k \). If \( a^k \neq e \) for all positive integers \( k \), then we say that the order of \( a \) is infinite and write \( o(a) = \infty \).

Here is a theorem which says that the order of an element \( a \) and the number of elements in \( \langle a \rangle \) are the same.

**Theorem 2.6:** Let \((G, \cdot)\) be any multiplicative group and let \( a \) be any element in \( G \). If the order of \( a \) is infinite, then the integral powers of \( a \) are all distinct, and \( \langle a \rangle \) contains infinitely many elements. If \( a \) has finite order \( k \), then \( \langle a \rangle \) contains exactly \( k \) elements, which are given distinctly in the list \( a^0, a^1, a^2, \ldots, a^{k-1} \).

2.4 **An application to the analysis of our puzzles.** The ideas of subgroups, and in particular subgroups generated by a few elements, have immediate applications to our analysis of the puzzles we have been studying. In particular, if you are looking at one of the puzzles that has \( n \) disks, we can think of the scrambles that we can get on the puzzle as permutations in \( S_n \). There is more relationship to the group
structure of $S_n$ going on, however. Specifically, the set of all of the permutations obtainable on a puzzle form a subgroup of $S_n$. We illustrate the principle with this theorem.

**Theorem 2.7:** Consider version $i$ of the Oval Track Puzzle with $n$ denoting the number of active disks. Let $R$ denote a single-position clockwise rotation, $R = (1, 2, 3, \ldots, n)$ and let $T$ denote the other “Do Arrows” permutation. The scrambles on the puzzle that are solvable are those that are in $<R, T>$, the subgroup of $S_n$ generated by the two basic puzzle moves, $R$ and $T$. The puzzle is completely solvable if and only if $<R, T> = S_n$.

**Exercises.**

*Sometimes we need to make use of specific information about a group to check whether subsets of interest to us are subgroups or not. For example, when we saw that the differentiable functions form a subgroup of the set of all functions from the real numbers to the real numbers, we were making use of properties that were quite specific in nature. However there are certain subsets which can be defined in any group which may or may not be subgroups. These first four exercises give you some examples. There are some of these that turn out to be subgroups in case the group is abelian (everything commutes with everything else) and may not be subgroups if the group is not abelian.*

2.1 **The center of a group.** Let $(G, \cdot)$ be any group. Define the center of $G$ to be the subset $Z(G)$ of $G$ consisting of all those elements of $G$ that commute with every element of $G$. Prove that $Z(G)$ is a subgroup of $G$.

2.2 **The centralizer of an element of a group.** Let $(G, \cdot)$ be any group and let $a$ be a fixed element of $G$. The centralizer of $a$ is defined to be the set $C_a$ of all elements of $G$ that commute with $a$. Prove that $C_a$ is a subgroup of $G$.

2.3 **The self-inverse elements.** Let $(G, \cdot)$ be any group and define $SI$ to be the set of those elements of $G$ that are self-inverse elements. That is, $SI = \{x \mid x \in G \text{ and } x = x^{-1}\}$. (a) Prove that if $G$ is an abelian group, then $SI$ is a subgroup of $G$. (b) Prove conversely that if $SI$ is a subgroup of $G$, then $G$ must be an abelian group. (c) Identify the self-inverse elements in the group $S_n$ where $n \geq 2$. Show why this set is never a subgroup of $S_n$ as long as $n \geq 2$. 
2.4 The elements of a fixed finite order. Let $(G, \cdot)$ be any group. Fix a positive integer $n$, and define $H_n$ to be the subset of $G$ consisting of the elements which have $n$-th powers that are the identity. That is, $H_n = \{x | x \in G, x^n = e\}$. (a) Prove that if $G$ is an abelian group, then $H_n$ is a subgroup of $G$. (b) Explore what can happen when $G$ is not abelian, showing that there are times when $H_n$ is a subgroup and other times when it is not.

This next group of two problems explore subgroups of a specific group that is nonabelian, but which we can easily visualize. The group is the set $L$ of all the linear permutations of the real numbers $\mathbb{R}$. Specifically, $L$ is the set of all functions from $\mathbb{R}$ to $\mathbb{R}$ that can be expressed by a linear function $f_{a,b}(x) = ax + b$, where the slope, $a$, is nonzero. That is, $L = \{f_{a,b} \mid a \text{ and } b \text{ are in } \mathbb{R} \text{ and } a \neq 0\}$.

The operation on $L$ is composition of functions. You can check that if you compose two linear functions of nonzero slope, you get back a linear function of nonzero slope, and the result is given by this formula:

$$f_{a,b} \circ f_{c,d} = f_{ac, ad+b}.$$ 

Also, if you take the inverse of a linear function of nonzero slope, the result is again a linear function of nonzero slope with the result given by this formula:

$$f_{a,b}^{-1} = f_{a^{-1}, -a^{-1}b}.$$ 

2.5 Explore whether these subsets of $L$ are subgroups.

(a) The set $H_1$ consisting of those linear functions that have slope 1 or -1.
(b) The set $H_2$ consisting of those linear functions that have rational slope.
(c) The set $H_3$ consisting of those linear functions that have integer slope.
(c) The set $H_4$ consisting of those linear functions that have y-intercept of 0.
(c) The set $H_5$ consisting of those linear functions that an integer as the y-intercept.

2.6 We can visualize each linear function with its graph. Using this form of visualization, describe each of the subsets in the previous exercise.