

Subgroups

Let G be a group. A nonempty subset S of G is a subgroup if it satisfies two conditions:

1. If $x \in S$ and $y \in S$ then $x \cdot y \in S$ (closure)
2. If $x \in S$ then $x^{-1} \in S$ (inverse closure)

Example 1

Is $\{e, b, b^2\}$ a subgroup of D_3 ? Let's consider closure. There are nine products to check because the left multiplier can be any of three elements and the same can be said of the right multiplier. These nine products are: $e \cdot e$, $e \cdot b$, $e \cdot b^2$, $b \cdot e$, $b \cdot b$, $b \cdot b^2$, $b^2 \cdot e$, $b^2 \cdot b$ and $b^2 \cdot b^2$. It is simple to verify that every result from these n products is an element of S . Let's consider inverse closure. There are only three calculations to execute: e^{-1} , b^{-1} and $(b^2)^{-1}$.

$$\begin{aligned}e^{-1} &= e \\ b^{-1} &= b^2 \\ (b^2)^{-1} &= b\end{aligned}$$

Each of these results is in S . $\therefore \{e, b, b^2\}$ **is** a subgroup of D_3 .

Example 2

Is $\{1, i, -i\}$ a subgroup of Q_8 ? Inverse closure is easy to verify:

$$\begin{aligned}1^{-1} &= 1 \\ i^{-1} &= -i \\ (-i)^{-1} &= i\end{aligned}$$

However, closure is violated. $i \cdot i$ is one of the products we must check. $i \cdot i = -1$ which is not an element of the given subset. $\therefore \{1, i, -i\}$ **is not** a subgroup of Q_8 .

Example 3

Let G be the group of all integers under addition. Let $S = \{\dots -4, -2, 0, 2, 4, \dots\}$. In other words, S is the set of all even integers. Is S a subgroup of G ? The sum of two even integers is an even integer establishing closure. Since the inverse of n is $-n$, the inverse of an even integer is an even integer. $\therefore S$ is a subgroup of G . Notice that the set of odd integers is not a subgroup of G .

Example 4

Let G be the set of all nonsingular 2×2 matrices. Is the set of matrices S of the form $\begin{pmatrix} a & 0 \\ x & a \end{pmatrix}$ where $a \neq 0$ (an example would be $\begin{pmatrix} -5 & 0 \\ 7 & -5 \end{pmatrix}$) a subgroup of G ? Examining this subset will be more difficult than the previous examples, but will truly reflect the difficulties posed when trying to prove that a subset is a subgroup. Notice that we do not restrict x . x may or may not equal 0.

Closure

Let $\begin{pmatrix} a & 0 \\ x & a \end{pmatrix}$ and $\begin{pmatrix} b & 0 \\ y & b \end{pmatrix}$ be elements of S (i.e. $a \neq 0$ and $b \neq 0$). Consider the product: $\begin{pmatrix} a & 0 \\ x & a \end{pmatrix} \cdot \begin{pmatrix} b & 0 \\ y & b \end{pmatrix} = \begin{pmatrix} ab & 0 \\ bx+ay & ab \end{pmatrix}$. Since a and b aren't 0, ab can't be 0. this result has all the characteristics of an element of S :

1. The main diagonal elements are equal and not 0.
2. The element in the first row, second column (the 1,2 position) is 0.
(Notice we have no interest in what appears in the 2,1 position).
 $\therefore S$ is closed under matrix multiplication.

Inverse Closure

To help establish inverse closure, let's review a simple way to compute the inverse of a 2×2 matrix which is discussed in most Linear Algebra courses. Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a nonsingular 2×2 matrix. The determinant of M is $ad - bc$ which can not equal 0. Let $ad - bc = D$. $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{D} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. This is a fairly easy pattern to remember.

Now let's pick an arbitrary element of S and compute its inverse.

$\begin{pmatrix} a & 0 \\ x & a \end{pmatrix}^{-1} = \frac{1}{a^2} \begin{pmatrix} a & 0 \\ -x & a \end{pmatrix} = \begin{pmatrix} \frac{1}{a} & 0 \\ -\frac{x}{a^2} & \frac{1}{a} \end{pmatrix}$ Note that $\frac{1}{a}$, $\frac{1}{a^2}$, and $-\frac{x}{a^2}$ are not undefined since the definition of S demands that $a \neq 0$.

Note further that $\begin{pmatrix} \frac{1}{a} & 0 \\ \frac{-x}{a^2} & \frac{1}{a} \end{pmatrix}$ meets all the requirements to be an element of S . $\therefore S$ is inverse closed. $\therefore S$ is a subgroup of the group of all 2×2 nonsingular matrices.

The requirements for a subset S to be a subgroup of a group G can be relaxed if G is finite. Consider the following:

Theorem: Let G be a finite group. Let S be a subgroup of G such that is $a, b \in S$ then $a \cdot b \in S$. S is a subgroup of G .

Proof: We only need to prove that if $x \in S$ then $x^{-1} \in S$. Since $x \in S$, $x \cdot x = x^2 \in S$ by closure. Similarly, x^3, x^4, \dots must also be in S . Construct the set $\{x, x^2, x^3, x^4, \dots\}$. Since each of the elements in this set are in G and since G is finite, there must be duplication in this set. Let $x^i = x^j$ where $i < j$. By an argument that we have become familiar with, $x^{i-j} = e$. Let $i - j = k$. $\therefore x^k = e$. If $k = 1$, $x = e$. $e^{-1} = e$ and x^{-1} is automatically in S . If $k > 1$, $x^k = x^{k-1} \cdot x$. $\therefore e = x^{k-1} \cdot x$. $\therefore x^{k-1} = x^{-1}$. Since x^{k-1} is in S , we know $x^{-1} \in S$. In both cases, $x^{-1} \in S$.

QED

Theorem: Let G be a group. Let S be a subgroup of G . e must be an element of S .

Proof: The thrust of this theorem is that the identity is an element of every subgroup of any group. The proof relies entirely upon the definition of a subgroup.

Let $x \in S$. By definition $x^{-1} \in S$. Since S is closed, $x \cdot x^{-1} \in S$. $\therefore e \in S$.

QED

Theorem: Let G be any group. $\{e\}$ is a subgroup of G and G is a subgroup of G .

Proof: The fact that $\{e\}$ is a subgroup of G relies upon two facts: $e^{-1} = e$ (inverse closure) and $e \cdot e = e$ (closure).

The fact that G is a subgroup of G relies upon the definition of a group. G has closure and every element in G has an inverse in G .

QED

Now we know that every group has at least two subgroups. However, $\{e\}$ and G are rather uninteresting subgroups. We will call these the trivial subgroups of G .

Let G be a group. Let S be a subgroup of G . Let $x \in G$. The symbol Sx denotes the set of all products of the form sx where $s \in S$. Sx is called the right coset of S in G generated by x . The symbol xS is defined similarly and is called the left coset of S in G generated by x . For example, let $G = D_4$. The set $S = \{e, ab\}$ is a subgroup of D_4 . The right coset of S in D_4 generated by a is Sa and equals the set $\{e \cdot a, ab \cdot a\} = \{a, b^3\}$. In fact, let's generate all right cosets of S in D_4 :

$$\begin{aligned} Se &= \{e, ab\} \\ Sa &= \{a, b^3\} \\ Sb &= \{b, ab^2\} \\ Sb^2 &= \{b^2, ab^3\} \\ Sb^3 &= \{b^3, a\} \\ Sab &= \{ab, e\} \\ Sab^2 &= \{ab^2, b\} \\ Sab^3 &= \{ab^3, b^2\} \end{aligned}$$

Notice that any two of the right cosets are equal (the order that the elements are written in a set is immaterial) or disjoint (have no elements in common). This will become an extremely important theorem shortly.

Let's also construct all left cosets of S in D_4 :

$$\begin{aligned} eS &= \{e, ab\} \\ aS &= \{a, b\} \\ bS &= \{b, a\} \\ b^2S &= \{b^2, ab^3\} \\ b^3S &= \{b^3, ab^2\} \\ abS &= \{ab, e\} \\ ab^2S &= \{ab^2, b^3\} \\ ab^3S &= \{ab^3, b^2\} \end{aligned}$$

Once again, two left cosets are either identical or disjoint. However, we can now add a new observation. The left coset generated by an element x in D_4 is not necessarily equal to the right coset generated by x . This becomes a major consideration in the next chapter.

Theorem: Let G be a group. Let S be a subgroup of G . Let x and y be arbitrary elements of G . Either $Sx = Sy$ or $Sx \cap Sy = \emptyset$.

Proof: If $Sx \cap Sy = \emptyset$ then we have nothing further to consider. Suppose $Sx \cap Sy \neq \emptyset$. Then there exists at least one element p in G such that $p \in Sx \cap Sy$.

$$\therefore p \in Sx \text{ and } p \in Sy$$

$$\therefore p = s_1x \text{ for some } s_1 \in S \text{ and } p = s_2y \text{ for some } s_2 \in S.$$

$$\therefore s_1^{-1}p = x \text{ for some } s_1 \in S \text{ and } s_2^{-1}p = y \text{ for some } s_2 \in S.$$

We will show that every element in Sx is also an element in Sy . Also, every element in Sy will be shown to be an element in Sx . This will establish that $Sx = Sy$.

Let q be an arbitrary element of Sx .

$$q = s_3x \text{ for some } s_3 \text{ in } S$$

$$\therefore q = s_3s_1^{-1}p$$

$$\therefore q = s_3s_1^{-1}s_2y$$

Since S is a subgroup, $s_3s_1^{-1}s_2 \in S$ which we will call s_4

$$\therefore q = s_4y \text{ for some } s_4 \in S$$

$$\therefore q \in Sy$$

At this point we know that $Sx \subseteq Sy$. Now let $t \in Sy$.

$$\therefore t = s_5y \text{ for some } s_5 \in S$$

$$\therefore t = s_5s_2^{-1}p$$

$$\therefore t = s_5s_2^{-1}s_1x$$

Again, because S is a subgroup, the last equation implies that $t \in Sx$.

$$\therefore Sx = Sy$$

QED

The fact that two right cosets are either disjoint or equal is only one key to an extremely important result in this chapter.

Suppose G is a finite group. Suppose S is a subgroup of G such that $o(S) = k$. Let the distinct elements of S be denoted $s_1, s_2, s_3, \dots, s_k$. We claim that every right (or left) coset generated by S in G also has k distinct elements. To prove this claim, let $x \in G$. $Sx = \{s_1x, s_2x, s_3x, \dots, s_kx\}$ The only way that Sx could not have k elements is if there exists duplication in the listing of Sx . But if $s_ix = s_jx$ then $s_i = s_j$ by RHC. $\therefore Sx$ also has k distinct elements. Now we are ready to prove one of the most important theorems in finite group theory.

Lagrange's Theorem: If G is a finite group and S is a subgroup of G then $o(S)$ is a divisor of $o(G)$.

Proof: If $o(S) = k$ then each right coset generated by S has k elements. Any two right cosets are either disjoint or equal. Every element x in G is in at least one coset. Namely, $x \in Sx$ since $x = ex$ and $e \in S$ (Recall that every subgroup contains the identity). If we construct all right cosets, there will be some that are duplicates of others. If we discard all duplicates, those that remain will contain every element of G and will have the property that any pair of them will be disjoint. However, each of the remaining distinct right cosets has the same number of elements (namely k). We have partitioned G into a disjoint collection of cosets each having k elements. This is only possible if $o(G) = k \cdot n$ where n is the number of distinct right cosets. $\therefore k$ is a divisor of $o(G)$ $\therefore o(S)$ is a divisor of $o(G)$.

QED

Now we have the information necessary to save time and effort in searching for subgroups within a given finite group. If our group has order 8, we need not search for subgroups of order 3, 5, 6 or 7 since these integers are not divisors of 8. We will use this information to find all subgroups of groups we have in our library. Remember that a subset of a finite group is a subgroup iff it is closed.

Example 1

Let's find all subgroups of D_4 . You should now consult your D_4 index card. The subgroups are closed subsets of orders 1, 2, 4 and 8.

Order 1	Order 2	Order 4	Order 8
$\{e\}$	$\{e, a\}$	$\{e, b, b^2, b^4\}$	D_4
	$\{e, b^2\}$	$\{e, a, b^2, ab^2\}$	
	$\{e, ab\}$	$\{e, b^2, ab, ab^3\}$	
	$\{e, ab^2\}$		
	$\{e, ab^3\}$		

Example 2

Let's find all subgroups of Z_{12} . They must be closed subsets of orders 1, 2, 3, 4, 6 and 12.

Order 1	Order 2	Order 3	Order 4	Order 6	Order 12
$[0]$	$\{[0], [6]\}$	$\{[0], [4], [8]\}$	$\{[0], [3], [6], [9]\}$	$\{[0], [2], [4], [6], [8], [10]\}$	Z_{12}

You should begin the process of finding all the subgroups of the groups in our library. You could list the subgroups on the back of the index card. You will notice many different patterns while doing this work. The nature of mathematics is such that patterns are usually significant, usually explored and usually reveal new insights.

We have proven that every finite group with even order has a non-trivial self invertible element. La Grange's Theorem can be used to explore finite groups with odd order. Suppose a finite group with odd order possessed a non-trivial self invertible element t . The subset $\{e, t\}$ would be closed under the group operator. Hence, $\{e, t\}$ would be a subgroup. However, the order of this subgroup would be 2. Since 2 is not a divisor of an odd integer, this subgroup can not exist. As a consequence, finite groups with odd order never possess non-trivial self invertible elements.

Let G be an arbitrary group. Let x be an element of G . The symbol $\langle x \rangle$ will represent the set $\{\dots, x^{-3}, x^{-2}, x^{-1}, e, x, x^2, x^3, \dots\}$. It is easy to verify that this set is a subgroup of G . We will call $\langle x \rangle$ the subgroup generated by x . if G is finite and $o(x) = n$ then $\langle x \rangle = \{e, x, x^2, \dots, x^{n-1}\}$. We have seen previously that if there is duplication in this set then $o(x)$ must be smaller than n . Therefore, $o(\langle x \rangle) = n$. By LaGrange's Theorem, n is a divisor of $o(G)$. This proves:

Theorem: If G is a finite group and $x \in G$ then $o(x)$ is a divisor of $o(G)$.

Suppose G is a finite group with order equal to a prime number. G can have no non-trivial subgroups since prime numbers don't possess non-trivial divisors. Is the converse true? Suppose G is a finite group of order n where $n > 1$. Suppose G has no non-trivial subgroups. Select x in G where $x \neq e$. As seen previously, $\langle x \rangle$ is a subgroup of G . Since G doesn't possess non-trivial subgroups and since $x \neq e$, $\langle x \rangle = G$. $\therefore G$ is cyclic. $\therefore G$ is isomorphic to \mathbb{Z}_n . The elements of G could be named $\{[0], [1], [2], \dots, [n-1]\}$. Is n a prime number? Suppose n is not prime. Then there exists positive integers a and b such that:

1. $a \cdot b = n$
2. $1 < a < n$ and $1 < b < n$.

Consider the order of the element $[a]$ in G . Since $\underbrace{[a] + [a] + \dots + [a]}_{b \text{ addends}}$
 $= [a \cdot b] = [0]$, the order of $[a]$ is less than or equal to b . This implies that $\langle [a] \rangle$ is a non-trivial subgroup of G . since this contradicts the fact that G doesn't have any non-trivial subgroups, n must be prime. we have proven:

Theorem: If G is a finite group with no non-trivial subgroups then G is isomorphic to \mathbb{Z}_p for some prime number p .

Let's consider the term "subgroup". The elements themselves form a subset of the original group. However, the term implies more than this fact. A subgroup of a group is a group itself. Remember that to be a group, a set with an operator must meet certain requirements. Suppose G is a group and S is a subgroup of G . The operator \star is well defined and associative on G and this is "inherited" by S . The fact that \star is closed on S and the fact that every element in S has its inverse also in S come from the definition of a subgroup. Finally, the fact that S possesses the identity is the subject of one of our theorems. Recall that $\{e, a, b^2, ab^2\}$ is a subgroup of D_4 . If we construct an operating table for this subgroup we obtain the following isomorphic copy of K_4 :

	e	a	b^2	ab^2
e	e	a	b^2	ab^2
a	a	e	ab^2	b^2
b^2	b^2	ab^2	e	a
ab^2	ab^2	b^2	a	e

In a sense, we could take the position that K_4 is "embedded" in D_4 . It is an interesting exercise to similarly consider operating tables for the other subgroups of D_4 .

Let's end this chapter by investigating a new family of groups. Given the elements in \mathbb{Z}_n , let's delete $[0]$ and consider the behavior of the remaining elements under multiplication. If an element $[k]$ has a multiplicative identity, then $[k]$ is called a unit. In \mathbb{Z}_9 , $[7]$ is a unit since $[7] \cdot [4] = [1]$ and $[4] \cdot [7] = [1]$. Notice that $[4]$ must be a unit also. Let's form the set of all units in \mathbb{Z}_n . This set is closed under multiplication. To prove this, let $[a]$ and $[b]$ be units. Let $[a]^{-1} = [c]$ and $[b]^{-1} = [d]$ where the inverse symbol refers to multiplication. Is $[a] \cdot [b]$ a unit? Consider $([a] \cdot [b]) \cdot ([d] \cdot [c])$. By associativity, the result of this product is $[1]$. Notice that $[1]$ is a unit in \mathbb{Z}_n for any n since $[1] \cdot [1] = [1]$. In fact, the units of \mathbb{Z}_n meet all of the conditions necessary to form a group. We will call this group U_n .

The elements in U_9 are $[1],[2],[4],[5],[7]$ and $[8]$. A chart for U_9 is as follows:

U_9	[1]	[2]	[4]	[5]	[7]	[8]
[1]	[1]	[2]	[4]	[5]	[7]	[8]
[2]	[2]	[4]	[8]	[1]	[5]	[7]
[4]	[4]	[8]	[7]	[2]	[1]	[5]
[5]	[5]	[1]	[2]	[7]	[8]	[4]
[7]	[7]	[5]	[1]	[8]	[4]	[2]
[8]	[8]	[7]	[5]	[4]	[2]	[1]

The elements of U_{12} are [1],[5], [7] and [11]. A chart for U_{12} is:

U_{12}	[1]	[5]	[7]	[11]
[1]	[1]	[5]	[7]	[11]
[5]	[5]	[1]	[11]	[7]
[7]	[7]	[11]	[1]	[5]
[11]	[11]	[7]	[5]	[1]

U_{12} is an isomorphic copy of K_4 . Could U_9 be an isomorphic copy of a group that we have already studied? we will return to this question in a later chapter.