Suppose that $G$ is a group and that $H \subseteq G$. If $H$ is also a group (under the same operation as $G$), then we say that $H$ is a **subgroup** of $G$. If $G$ is a group with identity element $e$, then $E = \{e\}$ is a subgroup of $G$ called the **trivial subgroup** of $G$. It is also true, for any group $G$, that $G$ is a subgroup of itself. If $H$ is a subgroup of $G$ with $H \neq G$, then $H$ is called a **proper subgroup** of $G$.

**Example 1** The set of even integers is a proper subgroup of the group of all integers under addition. The set of all multiples of 5 is also a proper subgroup of the integers under addition. In fact, if $k$ is any fixed integer, then

$$k \mathbb{Z} = \{kn \mid n \in \mathbb{Z}\} = \{\ldots, -3k, -2k, -k, 0, k, 2k, 3k, \ldots\}$$

is a subgroup of the integers under addition. Note that if $k = 0$, then we obtain the trivial subgroup $\{0\}$; whereas if $k = \pm 1$, then we obtain the entire group $\mathbb{Z}$. Thus, unless $k = \pm 1$, $k \mathbb{Z}$ is a proper subgroup of $\mathbb{Z}$.

**Example 2** Consider the multiplicative group $\mathbb{Q} - \{0\}$. A subgroup of this group is $H = \{-1, 1\}$. Another subgroup of $\mathbb{Q} - \{0\}$ is

$$H = \{2^n \mid n \text{ is an integer}\} = \{\ldots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \ldots\}.$$ 

To see this, note that $H$ is closed under multiplication because if $m$ and $n$ are any integers, then

$$2^m \cdot 2^n = 2^{m+n}.$$ 

Also, $H$ clearly satisfies the associative property (since $Q$ does and $H \subseteq Q$), $1 \in H$, and every member of $H$ has a multiplicative inverse in $H$. 

1
Example 3 Let us determine all of the subgroups of the group $Z_4 = \{0, 1, 2, 3\}$ under addition. Of course, $Z_4$ is a subgroup of $Z_4$ and we also have the trivial subgroup $\{0\}$. Suppose that 1 is in some subgroup, $H$, of $Z_4$. Then, since $H$ is closed (under addition), we see that $1+1 = 2 \in H$, $1+2 = 3 \in H$ and also $0 \in H$ because the identity element must be in $H$ (or because $1+3 = 0 \in H$). Thus, if $1 \in H$, then it must be true that $H = Z_4$. Now suppose that $H$ is a subgroup of $Z_4$ with $3 \in H$. Then $3+3 = 2 \in H$ and $3+2 = 1 \in H$ and we see once again that $H = Z_4$. The only non-trivial proper subgroup of $Z_4$ is $H = \{0, 2\}$.

Example 4 The group $U_8 = \{1, 3, 5, 7\}$ (under multiplication) has four non-trivial proper subgroups. They are $\{1\}$, $\{1, 3\}$, $\{1, 5\}$, and $\{1, 7\}$. Notice that $\{1, 3, 5\}$ is not a subgroup of $U_8$ because $3 \cdot 5 = 7$ so $\{1, 3, 5\}$ is not closed under multiplication. Likewise, $\{1, 3, 7\}$ and $\{1, 5, 7\}$ are not subgroups of $U_8$.

The proof of the following Proposition is left as homework.

Proposition 5 If $G$ is a group and $H_1$ and $H_2$ are subgroups of $G$, then $H_1 \cap H_2$ is a subgroup of $G$.

1 Cyclic Groups

A group, $G$, is said to be cyclic if there exists an element $a \in G$ such that $G = \{a^n \mid n \text{ is an integer}\}$. (Note that if $G$ is an additive group, then we would write $na$ instead of $a^n$.) If $a$ is an element or $G$ that has the property described above, then we say that $a$ is a generator of $G$ and we write $G = \langle a \rangle$.

Example 6 The group, $Z$, of integers under addition is a cyclic group with generator 1. This is because, for any integer $n$, we have $n = n \cdot 1$. Note that $-1$ is also a generator of $Z$. Thus we could write $Z = \langle 1 \rangle$ or $Z = \langle -1 \rangle$. $Z$ does not have any generators other than 1 and $-1$.

Example 7 The group, $2Z$, of even integers is cyclic with generator 2 because any even integer can be written in the form $n \cdot 2$ where $n$ is an integer. Thus $2Z = \langle 2 \rangle$. (It is also true that $2Z = \langle -2 \rangle$.)

2
Example 8 The group, \( Z_4 = \{0, 1, 2, 3\} \), under addition is cyclic with generator 1 because

\[
\begin{align*}
1 &= 1 \\
1 + 1 &= 2 \\
1 + 1 + 1 &= 3 \\
1 + 1 + 1 + 1 &= 0.
\end{align*}
\]

Thus every element of \( Z_4 \) can be written as \( n \cdot 1 \) for some integer \( n \). Does \( Z_4 \) have any other generators?

\[
\begin{align*}
2 &= 2 \\
2 + 2 &= 0 \\
2 + 2 + 2 &= 2 \\
\text{etc.}
\end{align*}
\]

shows that 2 is not a generator of \( Z_4 \).

\[
\begin{align*}
3 &= 3 \\
3 + 3 &= 2 \\
3 + 3 + 3 &= 1 \\
3 + 3 + 3 + 3 &= 0
\end{align*}
\]

shows that 3 is a generator of \( Z_4 \). Thus \( Z_4 = \langle 1 \rangle = \langle 3 \rangle \).

Exercise 9 It is clear that, for any integer \( n \geq 1 \), the additive group \( Z_n \) is cyclic with generator 1. Find all of the generators of \( Z_5 \), \( Z_6 \), \( Z_7 \), and \( Z_8 \). Can you make a general conjecture about the generators of \( Z_n \)?

Example 10 The group \( U_8 = \{1, 3, 5, 7\} \) under multiplication is not cyclic because \( 3^2 = 1 \), \( 5^2 = 1 \), and \( 7^2 = 1 \) so neither 3, nor 5, nor 7 generates \( U_8 \).

Even though not all groups are cyclic, all groups contain at least one cyclic subgroup – the subgroup \( E = \{e\} = \langle e \rangle \). In general, if \( G \) is any group and \( a \) is an element of \( G \), then \( \langle a \rangle \) is an abelian subgroup of \( G \) (even if \( G \) itself is not abelian). The subgroup \( \langle a \rangle \) is called the cyclic subgroup of \( G \) generated by \( a \). Of course, it may be the case that \( \langle a \rangle = G \) (in which case \( G \) itself is cyclic) or it may be the case that \( \langle a \rangle = \langle b \rangle \) for two different elements, \( a \) and \( b \), of \( G \).
Proposition 11 Let $G$ be a group and let $a \in G$. Then $\langle a \rangle = \{a^n \mid n \text{ is an integer}\}$ is an abelian subgroup of $G$.

Proof. Since, for any integers $m$ and $n$, we have $a^m a^n = a^{m+n}$, we see that $\langle a \rangle$ is closed under the operation of $G$. Also, since $G$ obeys the associative law, then so does $\langle a \rangle$ just by virtue of the fact that $\langle a \rangle \subseteq G$. In addition, $a^0 = e \in \langle a \rangle$, and for any member, $a^n$, of $\langle a \rangle$, we see that $a^{-n} \in \langle a \rangle$ and $a^{-n}$ is the inverse of $a^n$. This proves that $\langle a \rangle$ is a group (and hence a subgroup of $G$.) To see that $\langle a \rangle$ is an abelian group, note that for any two integers $m$ and $n$, we have $a^m a^n = a^{n+m}$.

Example 12 Consider the dihedral group $D_3$ whose Cayley table is shown below. Find the cyclic subgroups of $D_3$ that are generated by each of the members of $D_3$.

\[
\begin{array}{c|cccccccc}
* & R_0 & R_1 & R_2 & F_a & F_b & F_c \\
\hline
R_0 & R_0 & R_1 & R_2 & F_a & F_b & F_c \\
R_1 & R_1 & R_2 & R_0 & F_c & F_a & F_b \\
R_2 & R_2 & R_0 & R_1 & F_b & F_c & F_a \\
F_a & F_a & F_b & F_c & R_0 & R_1 & R_2 \\
F_b & F_b & F_c & F_a & R_2 & R_0 & R_1 \\
F_c & F_c & F_a & F_b & R_1 & R_2 & R_0 \\
\end{array}
\]

Solution: The subgroup generated by $R_0$ is $\langle R_0 \rangle = R_0$. For $R_1$ we have

\[
\begin{align*}
R_1^1 &= R_1 \\
R_1^2 &= R_2 \\
R_1^3 &= R_0
\end{align*}
\]

so

\[\langle R_1 \rangle = \{R_0, R_1, R_2\}.\]

Likewise we see that

\[\langle R_2 \rangle = \{R_0, R_1, R_2\}.\]

Now note that

\[
\begin{align*}
F_a^1 &= F_a \\
F_a^2 &= R_0
\end{align*}
\]
so

\[ \langle F_a \rangle = \{ R_0, F_a \} . \]

Likewise it can be seen that \( \langle F_b \rangle = \{ R_0, F_b \} \) and that \( \langle F_c \rangle = \{ R_0, F_c \} \). Thus \( D_3 \) has one cyclic subgroup of order three and three cyclic subgroups of order two. (The cyclic subgroup of order three is generated by two different elements of \( D_3 \).)

**Example 13** Consider the multiplicative group \( Q \setminus \{0\} \). Find the cyclic subgroup of \( Q \) generated by \( 1/2 \).

**Solution:** Observe that

\[
\left( \frac{1}{2} \right)^0 = 1 \\
\frac{1}{2} = 1 \\
\left( \frac{1}{2} \right)^2 = \frac{1}{4}
\]

etc.

and

\[
\left( \frac{1}{2} \right)^{-1} = 2 \\
\left( \frac{1}{2} \right)^{-2} = 4
\]

etc.

Thus

\[ \left\langle \frac{1}{2} \right\rangle = \left\{ \ldots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \ldots \right\} . \]

**Proposition 14** Suppose that \( G \) is a group of finite order with identity element \( e \) and suppose that \( a \in G \). Then there exists an integer \( k > 0 \) such that \( a^k = e \).

**Proof.** If \( a = e \), then \( a^1 = e \). Thus suppose that \( a \neq e \). Since \( G \) is of finite order, it is not possible that all of the powers \( a^1, a^2, a^3, \ldots \) are different.
from one another (for then \( G \) would have infinite order). Therefore, there must exist some positive integers \( m \) and \( n \) with \( m > n \) such that \( a^m = a^n \). However this implies that \( a^{m-n} = a^0 = e \) (and note that \( m - n \) is a positive integer). This proves the assertion. 

**Corollary 15** If \( G \) is a group of finite order and \( H \) is a non–empty subset of \( G \) that is closed under the operation of \( G \), then \( H \) is a subgroup of \( G \).

**Proof.** It is clear that \( H \) satisfies the associative property (because \( G \) does and \( H \subseteq G \)). Also, \( H \neq \emptyset \) so there exists an element \( a \in H \). By the preceding Proposition (since \( G \) is of finite order), there must exist some positive integer \( k \) such that \( a^k = e \). Since \( H \) is closed under the operation of \( G \), it must therefore be true that \( e \in H \). Finally, we will show that if \( a \in H \), then \( a^{-1} \in H \). If \( a = e \), then \( a^{-1} = e \) so \( a^{-1} \in H \). If \( a \neq e \), the let \( k \) be a positive integer such that \( a^k = e \). Since \( a \neq e \), we know that \( k \geq 2 \). Also \( a^{-1} (a^k) = a^{-1} e \) and thus \( a^{-1} = a^{k-1} \). Since \( H \) is closed under the operation of \( G \), it must be the case that \( a^{k-1} \in H \). Therefore \( a^{-1} \in H \). This proves that \( H \) is a subgroup of \( G \). 

**Definition 16** Suppose that \( G \) is a group and suppose that \( a \in G \). We define the order of \( a \), denoted by \( |a| \), to be the order of the cyclic subgroup generated by \( a \). Thus \( |a| = |\langle a \rangle| \). (Note that \( |a| \) is either a positive integer or infinity.)

**Example 17** In Example 12, we learned that \( |R_1| = |R_2| = 3 \), whereas \( |F_a| = |F_b| = |F_c| = 2 \) in \( D_3 \). In Example 13, we learned that \( |1/2| = \infty \) in \( Q - \{0\} \).

The following corollary to Proposition 14 insures that if \( G \) is a group of finite order and \( a \in G \), then the entire subgroup \( \langle a \rangle \) is actually generated by positive powers of \( a \).

**Corollary 18** If \( G \) is a group of finite order and \( a \in G \), then

\[
\langle a \rangle = \{a^n \mid n \text{ is a positive integer} \}.
\]

**Proof.** We know (by definition) that

\[
\langle a \rangle = \{a^n \mid n \text{ is an integer} \}.
\]
Let
\[ A = \{a^n \mid n \text{ is a positive integer}\}. \]

We want to prove (under the assumption that \( G \) is of finite order) that \( \langle a \rangle = A \). First we will dispense with the case that \( a = e \). In this case, it is clear that \( \langle a \rangle = \{e\} \) and also that \( A = \{e\} \). Therefore \( \langle a \rangle = A \). Henceforth we assume that \( a \neq e \).

It is clear that \( A \subseteq \langle a \rangle \). Thus we only need to prove that \( \langle a \rangle \subseteq A \).

Let \( x \in \langle a \rangle \). Then there exists an integer \( m \) such that \( x = a^m \). If \( m > 0 \), then \( x \in A \). Thus suppose that \( m \leq 0 \). By Proposition 14, we know that there exists a positive integer \( k \) such that \( a^k = e \). Since \( k \) is a positive integer, we can find a positive integer \( r \) such that \( rk > -m \). (Note that \( -m \geq 0 \) because we are assuming that \( m \leq 0 \).) Since \( a^{rk} = (a^k)^r = e^r = e \), we obtain
\[ x = a^m = ea^m = a^{rk}a^m = a^{rk+m} \]
and since \( rk + m > 0 \) we see that \( x \in A \). Therefore \( \langle a \rangle \subseteq A \) and we have now proved that \( \langle a \rangle = A \). ■

2 Product Groups

Suppose that \( G_1 \) is a group with operation \(*_1\) and that \( G_2 \) is a group with operation \(*_2\). Then we can from a new group called the **product group** of \( G_1 \) and \( G_2 \) by using the Cartesian product \( G_1 \times G_2 \) as the underlying set and defining the operation, \(*\), on \( G_1 \times G_2 \) as follows:
\[ (a,b) * (c,d) = (a *_1 c, b *_2 d). \]

The group \( G_1 \times G_2 \) is also called the **direct product** of \( G_1 \) and \( G_2 \). If additive notation is in order (due to the fact that additive notation is being used for both \( G_1 \) and \( G_2 \)), then we usually write \( G_1 \oplus G_2 \) instead of \( G_1 \times G_2 \) and we call \( G_1 \oplus G_2 \) the **direct sum** of \( G_1 \) and \( G_2 \).

**Example 19** Let us consider the direct sum \( Z_2 \oplus Z_3 \). Since \( Z_2 = \{0,1\} \) and \( Z_3 = \{0,1,2\} \), the elements of \( Z_2 \oplus Z_3 \) are \((0,0)\), \((0,1)\), \((0,2)\), \((1,0)\), \((1,1)\),
and \((1, 2)\). The Cayley table for \(Z_2 \oplus Z_3\) is as follows:

<table>
<thead>
<tr>
<th>(*)</th>
<th>((0, 0))</th>
<th>((0, 1))</th>
<th>((0, 2))</th>
<th>((1, 0))</th>
<th>((1, 1))</th>
<th>((1, 2))</th>
</tr>
</thead>
<tbody>
<tr>
<td>((0, 0))</td>
<td>((0, 0))</td>
<td>((0, 1))</td>
<td>((0, 2))</td>
<td>((1, 0))</td>
<td>((1, 1))</td>
<td>((1, 2))</td>
</tr>
<tr>
<td>((0, 1))</td>
<td>((0, 1))</td>
<td>((0, 2))</td>
<td>((0, 0))</td>
<td>((1, 1))</td>
<td>((1, 2))</td>
<td>((1, 0))</td>
</tr>
<tr>
<td>((0, 2))</td>
<td>((0, 2))</td>
<td>((0, 0))</td>
<td>((0, 1))</td>
<td>((1, 2))</td>
<td>((1, 0))</td>
<td>((1, 1))</td>
</tr>
<tr>
<td>((1, 0))</td>
<td>((1, 0))</td>
<td>((1, 1))</td>
<td>((1, 2))</td>
<td>((0, 0))</td>
<td>((0, 1))</td>
<td>((0, 2))</td>
</tr>
<tr>
<td>((1, 1))</td>
<td>((1, 1))</td>
<td>((1, 2))</td>
<td>((0, 1))</td>
<td>((0, 2))</td>
<td>((0, 0))</td>
<td></td>
</tr>
<tr>
<td>((1, 2))</td>
<td>((1, 2))</td>
<td>((1, 0))</td>
<td>((1, 1))</td>
<td>((0, 2))</td>
<td>((0, 0))</td>
<td>((0, 1))</td>
</tr>
</tbody>
</table>

Let us compare the above group with the dihedral group \(D_3\) which is also a group of order 6 (and whose table is given in Example 12). \(D_3\) has one cyclic subgroup of order three and three cyclic subgroups of order two. In \(Z_2 \oplus Z_3\), we have

\[
2(0, 1) = (0, 2) \\
3(0, 1) = (0, 0)
\]

so \(|(0, 1)| = 3\). Likewise \(|(0, 2)| = 3\) and we see that \:\{(0, 0), (0, 1), (0, 2)\} is a subgroup of order 3 in \(Z_2 \oplus Z_3\).

Also

\[
2(1, 0) = (0, 0)
\]

so \(|(1, 0)| = 2\) and \:\{(0, 0), (1, 0)\} is a subgroup of order 2 in \(Z_2 \oplus Z_3\). However, \(Z_2 \oplus Z_3\) does not have any more cyclic subgroups of order 2 because

\[
2(1, 1) = (0, 2) \\
3(1, 1) = (1, 0) \\
4(1, 1) = (0, 1) \\
5(1, 1) = (1, 2) \\
6(1, 1) = (0, 0)
\]

and this shows that \(|(1, 1)| = 6\) and hence that \(Z_2 \oplus Z_3 = \langle(1, 1)\rangle\) (meaning that \(Z_2 \oplus Z_3\) is in fact a cyclic group). It can also be confirmed that \(|(1, 2)| = 6\). We conclude that \(D_3\) and \(Z_2 \oplus Z_3\) (although both groups of order 6) are essentially different from each other. \(Z_2 \oplus Z_3\) is cyclic and \(D_3\) is not. Also, \(Z_2 \oplus Z_3\) is abelian and \(D_3\) is not.
We note, referring to the above example, that $Z_2 \oplus Z_3$ has subgroups that are “copies” of $Z_2$ and $Z_3$. In particular $\{(0,0),(1,0)\}$ is a copy of $Z_2$ and $\{(0,0),(0,1),(0,2)\}$ is a copy of $Z_3$. This is always the case with direct products (or direct sums). In $G_1 \times G_2$ (with respective identity elements $e_1$ and $e_2$), the subgroup $\{(x,e_2) \mid x \in G_1\}$ is a copy of $G_1$ and the subgroup $\{(e_1,y) \mid y \in G_2\}$ is a copy of $G_2$. More generally, in a direct product $G_1 \times G_2 \times \cdots \times G_n$, the subgroup $\{(e_1,e_2,\ldots,x,\ldots,e_n) \mid x \in G_i\}$ is a copy of $G_i$. Because of this fact, for any two positive integers $m$ and $n$ such that $n$ is divisible by $m$, we can always construct a group of order $n$ that has a subgroup of order $m$.

**Example 20** Suppose that we would like to construct a group of order 24 that contains a copy of the Klein 4–Group, $K$. Since $|K| = 4$ and 24 is divisible by 4, then this construction is possible. We can choose any group of order 6, say $D_3$, and be assured that $D_3 \times K$ is a group of order 24 that contains a copy of $K$. (Of course, $D_3 \times K$ also contains a copy of $D_3$.)

We conclude with a theorem that gives the order of an element in a product group in terms of the orders of the components of this element in their respective groups.

**Theorem 21** Let $G_1$, $G_2$, \ldots, $G_n$ be groups of finite order and let $a_i \in G_i$ for each $i = 1,2,\ldots,n$. Then the order of the element $(a_1,a_2,\ldots,a_n)$ in the product group $G_1 \times G_2 \times \cdots \times G_n$ is the least common multiple of the orders of $a_1$, $a_2,\ldots,a_n$ in the respective groups $G_i$, $i = 1,2,\ldots,n$.

In order to prove Theorem 21, we will need a Lemma that is of interest in its own right.

**Lemma 22** Suppose that $G$ is group and suppose that $a \in G$ with $|a| = n$. Then $a^m = e$ if and only if $m$ is divisible by $n$.

**Proof.** Suppose that $m$ is divisible by $n$. Then $m = qn$ where $q$ is an integer. This implies that

$$a^m = a^{qn} = (a^n)^q = e^q = e.$$ 

Now suppose that $m$ is not divisible by $n$. Then $m \neq 0$ and $m \neq \pm n$. If $0 < m < n$, then $a^m \neq e$ because this would contradict the fact that $|a| = n$. 

9
If \( m > n \), then the Division Algorithm gives us integers \( q \) and \( r \) such that \( m = qn + r \) and \( 0 < r < n \). In this case we have

\[
a^m = a^{qn+r} = (a^n)^q a^r = e^q a^r = e a^r = a^r
\]

and we know that \( a^r \neq e \) (because \( 0 < r < n \)) and thus \( a^m \neq e \). Finally, if \( m < 0 \), then \(-m > 0\) and we thus know that \( a^{-m} \neq e \). But this implies that \( a^m \neq e \) (because if \( a^m = e \) then we must have \( a^{-m}a^m = a^{-m}e \) and hence \( e = a^{-m} \)).

We now give the proof of Theorem 21. We will prove the theorem only for the case of two groups, \( G_1 \) and \( G_2 \).

**Proof of Theorem 21:** Suppose that \( G_1 \) and \( G_2 \) are groups of finite order (with respective operations \(*_1\) and \(*_2\) and respective identity elements \( e_1 \) and \( e_2 \)) and suppose that \( a_1 \in G_1 \) and \( a_2 \in G_2 \). Suppose also that \(|a_1| = s\) and \(|a_2| = t\). We want to prove that \(|(a_1, a_2)| = \text{lcm}(s, t)\).

To begin, note that \( a_1^s = e_1 \) and \( a_2^t = e_2 \). Letting \( m = \text{lcm}(s, t) \), we obtain

\[
(a_1, a_2)^m = (a_1^m, a_2^m) = (e_1, e_2)
\]

(by the preceding lemma, because \( m \) is divisible by both \( s \) and \( t \)). To prove that \(|(a_1, a_2)| = m\), we must show that \((a_1, a_2)^n \neq (e_1, e_2)\) for any integer \( n \) such that \( 0 < n < m \). To this end, suppose that \( 0 < n < m \) and suppose that \((a_1, a_2)^n = (e_1, e_2)\). Then \((a_1^n, a_2^n) = (e_1, e_2)\) which means that \( a_1^n = e_1 \) and \( a_2^n = e_2 \). By the preceding lemma, it must then be the case that \( n \) is divisible by both \( s \) and \( t \) or, in other words, that \( n \) is a common multiple of \( s \) and \( t \). Since the least common multiple of any two numbers divides any common multiple of those two numbers, it must then be the case that \( n \) is divisible by \( m \). However this is a contradiction because \( 0 < n < m \). We thus conclude that \(|(a_1, a_2)| = m\).