15 Generated Groups. Direct Product

In this section, we discuss two procedures of building (sub)groups, namely, the (sub)groups generated by a subset of a given group and the direct product of two or more groups.

15.1 Finitely and Infinitely Generated Groups

The concept of generators can be extended from cyclic groups $\langle a \rangle$ to more complicated situations where a subgroup is generated by more than one element. It is easy to see that a cyclic group with generator $a$ is the smallest subgroup containing the set $S = \{a\}$. Can we extend groups generated by sets with more than one element? The answer is affirmative as suggested by the following theorem.

**Theorem 15.1**

Let $G$ be a group and $\mathcal{C}$ be the collection all subgroups of $G$. Then $\cap_{H \in \mathcal{C}} H$ is a subgroup of $G$.

**Proof.** Let $K = \cap_{H \in \mathcal{C}} H$. Since $e$ belongs to all the subgroups of $G$ then $e \in K$ so that $K \neq \emptyset$. Now, let $a, b \in K$. Then $a \in H$ and $b \in H$ for all subgroups $H$ of $G$. But then $a \in H$ and $b^{-1} \in H, \forall H \in \mathcal{C}$. Since every $H$ in $\mathcal{C}$ is closed under multiplication then $ab^{-1} \in H, \forall H \in \mathcal{C}$. That is, $ab^{-1} \in K$. By Theorem 7.5, $K$ is a subgroup of $G$. ■

**Theorem 15.2**

Let $G$ be a group and $S \subseteq G$. Let $\mathcal{C}$ be the collection of all subgroups of $G$ containing $S$. Then the set $\langle S \rangle = \cap_{H \in \mathcal{C}} H$ satisfies the following:

(i) $\langle S \rangle$ is a subgroup of $G$ containing $S$.
(ii) For every $H \in \mathcal{C}$, $\langle S \rangle \subseteq H$.

Thus, $\langle S \rangle$ is the smallest subgroup of $G$ containing $S$. 

1
Proof.
(i) Note that since \( S \subseteq G \) then \( G \in \mathcal{C} \). Thus, \( \mathcal{C} \neq \emptyset \). The fact that \(< S >\) is a subgroup of \( G \) follows from Theorem 15.1. Since \( S \subseteq H \) for all \( H \in \mathcal{C} \) then \( S \subseteq \cap_{H \in \mathcal{C}} H \). That is, \( S \subseteq < S > \).
(ii) Let \( H \in \mathcal{C} \). If \( x \in < S > \) then \( x \in \cap_{H \in \mathcal{C}} H \) and in particular, \( x \in H \). Hence, \(< S > \subseteq H \).

Theorem 15.3
\(< S >\) is the only subgroup of \( G \) that satisfies conditions (i) and (ii) of Theorem 15.2

Proof.
Suppose that \( K \) is a subgroup of \( G \) satisfying conditions (i) and (ii) of the previous theorem. We will show that \( K = < S > \). Since \( < S > \) is a subgroup containing \( S \) then by (ii), we have \( < S > \subseteq K \). Also, since \( K \) is a subgroup of \( G \) containing \( S \) then by condition (ii) again, we have \( K \subseteq < S > \). Thus, \(< S > = K \).

Definition 15.1
If \( G \) is a group and \( S \subseteq G \) then the subgroup \(< S >\) is called the **subgroup of \( G \) generated by \( S \)**. If \( G = < S > \), then we say \( S \) generates \( G \); and the elements in \( S \) are called **generators**. For \( S = \{a_1, a_2, \ldots, a_n\} \) we write \(< S > = < a_1, a_2, \ldots, a_n > \).

Example 15.1
Consider the subgroup of \( S_4 \) generated by \( S = \{(1432), (24)\} \). Then
\(< S > = \{(1), (1432), (24), (14)(23), (1234), (12)(34), (13)(24), (13)\} \).

The following theorem characterizes the elements of \(< S >\).

Theorem 15.4
Let \( G \) be a group and \( S \subseteq G \). Then \(< S >\) consists of finite products of elements of \( S \) and inverses of elements of \( S \). That is, if \( K = \{a_1^{s_1}a_2^{s_2} \cdots a_k^{s_k}, a_i \in S, s_i = \pm 1\} \) then \(< S > = K \).

Proof.
The proof is by double inclusions. By closure, \( K \subseteq < S > \). It remains to show that \(< S > \subseteq K \). Since each element of \( S \) is in \( K \) then \( S \subseteq K \).
We will show that $K$ is a subgroup of $G$. Indeed, if $x = a_1^{s_1} a_2^{s_2} \cdots a_k^{s_k}$ and $y = b_1^{t_1} b_2^{t_2} \cdots b_m^{t_m}$ are two elements in $K$ then
\[
xy^{-1} = (a_1^{s_1} a_2^{s_2} \cdots a_k^{s_k})(b_1^{t_1} b_2^{t_2} \cdots b_m^{t_m})^{-1} \\
= (a_1^{s_1} a_2^{s_2} \cdots a_k^{s_k})(b_m^{-t_m} \cdots b_2^{-t_2} b_1^{-t_1}) \\
= a_1^{s_1} a_2^{s_2} \cdots a_k^{s_k} b_m^{-t_m} \cdots b_2^{-t_2} b_1^{-t_1}
\]
Thus, $xy^{-1}$ is a product of elements of $S$ and/or inverses of elements of $S$. Hence, $xy^{-1} \in K$. By Theorem 7.5, $K$ is a subgroup of $G$. By Theorem 15.2(ii), $< S > \subseteq K$. Hence, $< S > = K$. □

The next theorem provides a condition under which two groups generated by different sets are equal.

**Theorem 15.5**

Let $T_1$ and $T_2$ be subsets of a group $G$. Then

\[
<T_1> = <T_2> \text{ if and only if } T_1 \subseteq <T_2> \text{ and } T_2 \subseteq <T_1>
\]

**Proof.**

Suppose first that $<T_1> = <T_2>$. Since $T_1 \subseteq <T_1>$ and $<T_1> = <T_2>$ then $T_1 \subseteq <T_2>$. Similarly, $T_2 \subseteq <T_1>$.

Conversely, suppose that $T_1 \subseteq <T_2>$ and $T_2 \subseteq <T_1>$. By Theorem 15.2(ii), we have $<T_1> \subseteq <T_2>$ and $<T_2> \subseteq <T_1>$. Hence, $<T_1> = <T_2>$. □

**Example 15.2**

Consider $(\mathbb{Z}, +)$. Since $\{3\} \subseteq <9, 12>$ ($3 = 12 + (-9)$) and $\{9, 12\} \subseteq <3>$ then by the previous theorem we have $<9, 12> = <3>$. □

**Example 15.3**

In $S_4$ we have that
\[
\begin{align*}
(124) &= (123)(12)(34)(123) \\
(234) &= (132)(12)(34) = (123)^{-1}(12)(34) \\
(123) &= (124)(234) \\
(12)(34) &= (234)(124)^{-1}
\end{align*}
\]

Thus, we conclude that $\{(124), (134)\} \subseteq <(123), (12)(34)>$ and $\{(123), (12)(34)\} \subseteq <(124), (134)>$. Hence, by Theorem 15.5, we have $<(124), (234)> = <(123), (12)(34)>$. □
15.2 Direct Product of Groups.

In this section we keep building examples of groups. By defining a binary operation on the Cartesian product of two groups we obtain the group known as the direct product of the two groups.

Let $H$ and $K$ be two arbitrary groups and let $H \times K$ be the Cartesian product of $H$ and $K$. In set-builder notation

$$H \times K = \{(h, k) : h \in H \text{ and } k \in K\}.$$ 

Equality in $H \times K$ is defined by $(h, k) = (h', k')$ if and only if $h = h'$ and $k = k'$.

Define multiplication on $H \times K$ as follows:

$$(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2)$$

The set $H \times B$ is a group under the above multiplication as shown in the next theorem.

**Theorem 15.6**

Multiplication on $H \times K$ satisfies the following properties:

(i) $H \times K$ is closed under multiplication.
(ii) Multiplication is associative.
(iii) $(e_H, e_K)$ is the identity element.
(iv) For each $(h, k) \in H \times K$ we have $(h, k)^{-1} = (h^{-1}, k^{-1})$.

**Proof.**

(i) We must show that the rule on $(H \times K) \times (H \times K) \rightarrow H \times K$ defined by $((h, k), (h', k')) \rightarrow (hh', kk')$ is a mapping. Indeed, if $((h_1, k_1), (h'_1, k'_1)) = ((h_2, k_2), (h'_2, k'_2))$ then $(h_1, k_1) = (h_2, k_2)$ and $(h'_1, k'_1) = (h'_2, k'_2)$. Thus, $h_1 = h_2, k_1 = k_2, h'_1 = h'_2$, and $k'_1 = k'_2$. Therefore, $h_1h'_1 = h_2h'_2$ and $k_1k'_1 = k_2k'_2$. Hence, $(h_1h'_1, k_1k'_1) = (h_2h'_2, k_2k'_2)$. So multiplication is a binary operation.

(ii) Multiplication on $H \times K$ is associative since multiplication is associative as operation on $H$ and $K$.

$$(h_1, k_1)(h_2, k_2)(h_3, k_3) = (h_1, k_1)(h_2h_3, k_2k_3) = (h_1(h_2h_3), k_1(k_2k_3)) = ((h_1h_2)h_3, (k_1k_2)k_3) = (h_1h_2, k_1k_2)(h_3, k_3) = [((h_1, k_1)(h_2, k_2))(h_3, k_3)$$
(iii) Let \((h, k) \in H \times K\). Since \(he_H = e_H h = h\) and \(ke_K = e_K k = k\) then 
\((he_H, ke_K) = (e_H h, e_K k) = (h, k)\). Hence, \((h, k)(e_H, e_K) = (e_H, e_K)(h, k) = (h, k)\). That is, \((e_H, e_K)\) is the identity element of \(H \times K\).

(iv) Let \((h, k) \in H \times K\). Since \(hh^{-1} = h^{-1}h = e_H\) and \(kk^{-1} = k^{-1}k = e_K\) then 
\((hh^{-1}, kk^{-1}) = (e_H, e_K)\). That is, \((h, k)(h^{-1}, k^{-1}) = (e_H, e_K)\). Similarly, 
\((h^{-1}, k^{-1})(h, k) = (e_H, e_K)\) so that \((h, k)\) is invertible with inverse \((h^{-1}, k^{-1})\).

**Definition 15.2**
By the above theorem, \(H \times K\) is a group, called the **direct product** of the groups \(H\) and \(K\).

**Example 15.4**
If \(Z_3 = \{[0], [1], [2]\}\) and \(S_2 = \{(1), (12)\}\) then 
\[Z_3 \times S_2 = \{([0], (1)), ([1], (1)), ([2], (1)), ([0], (12)), ([1], (12)), ([2], (12))\}\]

For example,
\[[[1], (12)][[2], (1)] = ([1] \oplus [2], (12)(1)) = ([0], (12))\]

Some of the subgroups of \(H \times K\) can be constructed as follows.

**Theorem 15.7**
The sets 
\[H \times \{e_K\} = \{(h, e_K) : h \in H\}\]
and 
\[\{e_H\} \times K = \{(e_H, k) : k \in K\}\]
are subgroups of \(H \times K\).

**Proof.**
We prove that \(H \times \{e_K\}\) is a subgroup of \(H \times K\) and we leave the second part of the theorem as an exercise for the reader. See Exercise ??

Since \((e_H, e_K) \in H \times \{e_K\}\) then \(H \times \{e_K\} \neq \emptyset\). Let \((h_1, e_K)\) and \((h_2, e_K)\) be two elements of \(H \times \{e_K\}\). Then
\[(h_1, e_K)(h_2, e_K)^{-1} = (h_1, e_K)(h_2^{-1}, e_K) = (h_1 h_2^{-1}, e_K) \in H \times \{e_K\}\]
since \(h_1 h_2^{-1} \in H\). Hence, by Theorem 7.5, \(H \times \{e_K\}\) is a subgroup of \(H \times K\).

**Remark 15.1**
By the Principle of Counting, if \(H\) and \(K\) are finite sets then \(|H \times K| = |H| \cdot |K|\).