Chapter 3

Elementary Group Theory

3.1 Structure of a Group

Group: A Group \((G, \oplus)\) is a set \(G\), along with a binary operation \(\oplus\) such that:

- Closure: It is closed under the binary operation: \((a \oplus b) \in G\) \(\forall a, b \in G\)

- Associative: The binary operation on the elements of \(G\) is associative: \(a \oplus (b \oplus c) = (a \oplus b) \oplus c\) \(\forall a, b, c \in G\)

- Identity: \(\exists\) an unique element \(e \in G\) such that: \(a \oplus e = e \oplus a = a\) \(\forall a \in G\). \(e\) is called the Identity element of \(G\).

- Inverse: \(\exists\) \(b \in G\) such that: \(ab = ba = e\) \(\forall a, b \in G\) where \(e\) is the Identity element of \(G\). \(b\) is called the inverse\(^1\) of \(a\) denoted as \(a^{-1}\).

Abelian: A group is called Abelian if, in addition to the above, the below property also holds:

- Commutative: \(a \oplus b = b \oplus a\) \(\forall a, b \in G\).

Order of a Group: The order of a group \((G, \oplus)\), denoted as \(|(G, \oplus)|\) is the cardinality of the set \(G\): \(|(G, \oplus)| = \#G\). Order of an element of the group: The order of an element \(g \in (G, \oplus)\) is \(n\) where \(g^n = e\).

3.1.1 Cayley Table

As the group is defined along with a binary operation \(\oplus\), we need to define this operation for every pair of elements in \(G\). To do this in a compact manner we have the following table.

\(^1\)Note that the inverse of an element depends upon the individual element and is not unique for a group, unlike the identity element.
Constructing the Cayley Table

Note that:

1. \( a \circ b = a \circ c \) implies \( b = c \) \( \forall a, b, c \in G \).
   Proof: Pre-Multiplying \( a^{-1} \) on both sides: \( a^{-1} \circ (a \circ b) = a^{-1} \circ (a \circ c) \). Since \( \exists \) a unique identity \( e \), \( a^{-1}a = e \ \forall a \in G \). Hence \( e \circ b = e \circ c \Rightarrow b = c \). Hence the result a binary operation on two elements will produce distinct results, unless they are same. Since along a particular row (or a particular column), each pair of elements involved in the binary operation is distinct, so is the result of the binary operation. Hence each element along a particular row (or column) is unique, as there are \#G positions along a row (or column).

2. Now in the previous case, putting \( a \rightarrow a^{-1} \) and \( c \rightarrow b^{-1} \), we see that \( a \circ a^{-1} = a \circ b^{-1} \) implies \( a^{-1} = b^{-1} \). Hence each element in \( G \) has a unique inverse.

3. \( \forall a, b \in G \) for which \( [a, b] = 0 \), as \( a \circ b = b \circ a \), \((a \circ b)\) is symmetric w.r.t the diagonal. Since \( \forall a \in G \), \([a, a^{-1}] = 0 \) and \((a \circ a^{-1}) = e \), all \( e \)'s are placed symmetric w.r.t the diagonal.

We now take a fixed example. Consider \( G = \{e, a, b, c, d, f\} \) with the binary operation \(' \). Let us construct the cayley table for \((G, \cdot)\).

1. As there are 5 elements (apart from \( e \)) and each of them must have an unique inverse, we see that (since there are an odd number of elements) at least one of them must be its own inverse. Just by choice we take \( a, b, c \) to be thier own inverses: \( a^{-1} = a \), \( b^{-1} = b \), \( c^{-1} = c \). For the other two elements \( d \) and \( f \), we assume them to be inverses of each other: \( d^{-1} = f \) \& \( f^{-1} = d \). Hence \( a \cdot a = b \cdot b = c \cdot c = d \cdot f = f \cdot d = e \).
   We now begin by placing \( e \)'s. Notice that they are symmetric about the diagonal.

2. Also note that \( g \cdot e = g \ \forall g \in G \). Hence the first row and first column are trivially filled.

3. Just by choice, we take \( a \cdot b = c \). From this, we get: \( a \cdot b = c \) \( (3.1) \)

\[
\begin{align*}
a \cdot c &= a \cdot (a \cdot b) \\
&= (a \cdot a) \cdot b \\
&= b \\
a \cdot c &= b \\
\end{align*}
\]

using (eq. 3.2): \( b \cdot c = (a \cdot c) \cdot c \) \( (3.2) \)

\[
\begin{align*}
a \cdot (c \cdot c) \\
&= a \\
b \cdot c &= a \\
\end{align*}
\]
4. Notice that the first row has two vacant positions. Using (statement 1), these two positions must be filled by \(d\) and \(f\). Hence consider the following two possibilities:

- **\(a \cdot d = d\):**

\[
\begin{align*}
  d &= a \cdot d \\
  d \cdot f &= (a \cdot d) \cdot f \\
  e &= a \cdot (d \cdot f) \\
  \therefore e &= a
\end{align*}
\]

The above statement is incorrect as it states that the identity element is not unique.

- **Hence the only other option is \(a \cdot d = f\).**

\[
\begin{align*}
  f &= a \cdot d \\
  f \cdot f &= (a \cdot d) \cdot f \\
  &= a \cdot (d \cdot f) \\
  &= a \therefore f \cdot f &= a \tag{3.5}
\end{align*}
\]

Using (eq. 3.4):

\[
\begin{align*}
  f \cdot d &= (a \cdot d) \cdot d \\
  &= a \cdot (d \cdot d) \\
  e &= a \cdot (d \cdot d) \\
  a \cdot e &= a \cdot (a \cdot (d \cdot d)) \\
  &= (a \cdot a) \cdot (d \cdot d) \\
  a &= d \cdot d \\
  \therefore d \cdot d &= a \tag{3.6}
\end{align*}
\]

Using (eq. 3.6): 

\[
\begin{align*}
  a \cdot (f \cdot d) &= d \cdot d \\
  &= (a \cdot (f \cdot d)) \cdot d \cdot f \\
  &= (a \cdot f) \cdot (d \cdot f) \\
  &= (a \cdot f) \cdot (d \cdot f) \\
  a \cdot f &= d \\
  \therefore a \cdot f &= d \tag{3.7}
\end{align*}
\]

5. Similarly, we need to determine: \((c \cdot a), (c \cdot b)\) and \((b \cdot a)\):

Using (eq. 3.1):

\[
\begin{align*}
  c \cdot a &= (a \cdot b) \cdot a \\
  &= a \cdot (b \cdot a) \\
  a \cdot (c \cdot a) &= (a \cdot a) \cdot (b \cdot a) \\
  Using \ a \cdot c = c \cdot a: \ c &= (b \cdot a) \therefore b \cdot a &= c \tag{3.8}
\end{align*}
\]

6. Hence the first row elements as well as their symmetric counterparts are determined. Notice that the positions marked by \(♣\) have to be filled either with \(d\) or \(f\) as the row containing them has the other symbols. But neither can be used as the column containing each has both \(d\) and \(f\). This states that the initial assumption \(a \cdot b = c\) is wrong.
Table 3.2: Cayley Table for $G = \{e, a, b, c, d, f\}$. Positions marked as ‘−’ have not yet been filled.

<table>
<thead>
<tr>
<th></th>
<th>$e$</th>
<th>$a$</th>
<th>$b$</th>
<th>$c$</th>
<th>$d$</th>
<th>$f$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td>$e$</td>
<td>$a$</td>
<td>$b$</td>
<td>$c$</td>
<td>$d$</td>
<td>$f$</td>
</tr>
<tr>
<td>$a$</td>
<td>$a$</td>
<td>$e$</td>
<td>$c$</td>
<td>$b$</td>
<td>$f$</td>
<td>$d$</td>
</tr>
<tr>
<td>$b$</td>
<td>$b$</td>
<td>$c$</td>
<td>$e$</td>
<td>$a$</td>
<td>$\bullet$</td>
<td>$\bullet$</td>
</tr>
<tr>
<td>$c$</td>
<td>$c$</td>
<td>$-$</td>
<td>$-$</td>
<td>$e$</td>
<td>$-$</td>
<td>$-$</td>
</tr>
<tr>
<td>$d$</td>
<td>$d$</td>
<td>$-$</td>
<td>$-$</td>
<td>$-$</td>
<td>$-$</td>
<td>$e$</td>
</tr>
<tr>
<td>$f$</td>
<td>$f$</td>
<td>$-$</td>
<td>$-$</td>
<td>$-$</td>
<td>$e$</td>
<td>$a$</td>
</tr>
</tbody>
</table>

7. Notice that $a \cdot b = a$, $a \cdot b = b$ are invalid as we would then get $e = a$ and $e = b$ respectively. With $a \cdot b = c$ also ruled out, we see that the only two options are $a \cdot b = d$ and $a \cdot b = f$. Let us take $a \cdot b = d$. With this we have:

\[
\begin{align*}
    a \cdot b &= d \\
    \text{Using (eq. 3.9):} \quad a \cdot (a \cdot b) &= a \cdot d \\
    b &= a \cdot d \quad \therefore a \cdot d = b \\
    \text{Using (eq. 3.10):} \quad (a \cdot b) \cdot b &= d \cdot b \\
    a &= d \cdot b \quad \therefore d \cdot b = a \\
    \text{Using (eq. 3.11):} \quad b \cdot f &= (a \cdot d) \cdot f \\
    b \cdot f &= a \quad \therefore b \cdot f = a \\
    \text{Using (eq. 3.12):} \quad b \cdot (b \cdot f) &= b \cdot a \\
    f &= b \cdot a \quad \therefore b \cdot a = f \\
    \text{Using (eq. 3.13):} \quad (b \cdot a) \cdot a &= f \cdot a \\
    b &= f \cdot a \quad \therefore f \cdot a = b
\end{align*}
\]

Filling the table now gives:

Table 3.3: Cayley Table for $G = \{e, a, b, c, d, f\}$. Positions marked as ‘−’ have not yet been filled.

<table>
<thead>
<tr>
<th></th>
<th>$e$</th>
<th>$a$</th>
<th>$b$</th>
<th>$c$</th>
<th>$d$</th>
<th>$f$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td>$e$</td>
<td>$a$</td>
<td>$b$</td>
<td>$c$</td>
<td>$d$</td>
<td>$f$</td>
</tr>
<tr>
<td>$a$</td>
<td>$a$</td>
<td>$e$</td>
<td>$d$</td>
<td>$-$</td>
<td>$b$</td>
<td>$-$</td>
</tr>
<tr>
<td>$b$</td>
<td>$b$</td>
<td>$f$</td>
<td>$e$</td>
<td>$-$</td>
<td>$-$</td>
<td>$a$</td>
</tr>
<tr>
<td>$c$</td>
<td>$c$</td>
<td>$-$</td>
<td>$-$</td>
<td>$e$</td>
<td>$-$</td>
<td>$-$</td>
</tr>
<tr>
<td>$d$</td>
<td>$d$</td>
<td>$-$</td>
<td>$a$</td>
<td>$-$</td>
<td>$-$</td>
<td>$e$</td>
</tr>
<tr>
<td>$f$</td>
<td>$f$</td>
<td>$b$</td>
<td>$-$</td>
<td>$-$</td>
<td>$e$</td>
<td>$-$</td>
</tr>
</tbody>
</table>
8. Notice that in the row corresponding to \( a \), we have two vacancies for \( a \cdot c \) and \( a \cdot f \). These must be filled using \( c \) or \( f \), as the other elements are already contained in this row. Also as \( a \cdot c \neq c \) (for if it was, then we would have \( e = a \), which is incorrect), the only assignments for the vacancies are:

\[
\begin{align*}
  a \cdot c &= f \\
  a \cdot f &= c
\end{align*}
\]

Using (eq. 3.15):

\[
(a \cdot c) \cdot c = f \cdot c
\]

\[
a = f \cdot c \quad \therefore f \cdot c = a
\]  

(3.17)

Using (eq. 3.16):

\[
(a \cdot f) \cdot d = c \cdot d
\]

\[
a = c \cdot d \quad \therefore c \cdot d = a
\]  

(3.18)

Using (eq. 3.18):

\[
c \cdot (c \cdot d) = c \cdot a
\]

\[
d = c \cdot a \quad \therefore c \cdot a = d
\]  

(3.19)

Using (eq. 3.20):

\[
(c \cdot a) \cdot a = d \cdot a
\]

\[
c = d \cdot a \quad \therefore d \cdot a = c
\]  

(3.20)

Filling the table, we get:

Table 3.4: Cayley Table for \( G = \{e, a, b, c, d, f\} \). Positions marked as ‘−’ have not yet been filled.

<table>
<thead>
<tr>
<th>X</th>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>f</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td>f</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>e</td>
<td>d</td>
<td>f</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>f</td>
<td>e</td>
<td>–</td>
<td>–</td>
<td>a</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>d</td>
<td>–</td>
<td>e</td>
<td>a</td>
<td>–</td>
</tr>
<tr>
<td>d</td>
<td>d</td>
<td>c</td>
<td>a</td>
<td>–</td>
<td>–</td>
<td>e</td>
</tr>
<tr>
<td>f</td>
<td>f</td>
<td>b</td>
<td>–</td>
<td>a</td>
<td>e</td>
<td>–</td>
</tr>
</tbody>
</table>

9. Notice that in the row corresponding to \( b \), there are two vacancies for \( b \cdot c \) and \( b \cdot d \) which must be filled using \( c \) and \( d \) as other elements in this row contain the rest of the elements. The option of putting \( b \cdot c = c \) (and hence \( b \cdot d = d \)) is ruled out since we will then get \( b = e \). Hence the only option of filling the two positions is to put:

\[
\begin{align*}
  b \cdot c &= d \\
  b \cdot d &= c
\end{align*}
\]

Using (eq. 3.21):

\[
(b \cdot c) \cdot c = d \cdot c
\]

\[
b = d \cdot c \quad \therefore d \cdot c = b
\]  

(3.23)

Now, the only vacant position in the row corresponding to \( d \) (for \( d \cdot d \)) must be filled with \( f \).

\[
\begin{align*}
  d \cdot d &= f
\end{align*}
\]

Using (eq. 3.22):

\[
(b \cdot d) \cdot f = c \cdot f
\]

\[
b = c \cdot f \quad \therefore c \cdot f = b
\]  

(3.25)

Finally, in the row corresponding to \( f \), the only vacancy (for \( f \cdot f \)) must be replaced by \( d \).

\[
\begin{align*}
  f \cdot f &= d
\end{align*}
\]

(3.26)
3.1. STRUCTURE OF A GROUP

Hence we have the final Cayley table:

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>f</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td>f</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>e</td>
<td>d</td>
<td>f</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>f</td>
<td>e</td>
<td>d</td>
<td>c</td>
<td>a</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>d</td>
<td>f</td>
<td>e</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>d</td>
<td>d</td>
<td>c</td>
<td>a</td>
<td>b</td>
<td>f</td>
<td>e</td>
</tr>
<tr>
<td>f</td>
<td>f</td>
<td>b</td>
<td>c</td>
<td>a</td>
<td>e</td>
<td>d</td>
</tr>
</tbody>
</table>

Table 3.5: Final Cayley Table for $G = \{e, a, b, c, d, f\}$.

3.1.2 Subgroups

Subgroup: $(H, \circlearrowleft)$ is a subgroup of $(G, \circlearrowleft)$ if $H \subseteq G$ and $(H, \circlearrowleft)$ satisfies the group properties. It is called an Abelian subgroup if it also satisfies the commutative law.

We can now infer few general properties:

- Every subgroup of a group contains the identity element of the group. As $(H, \circlearrowleft)$ is also a group, it has an identity element. Moreover since the identity element of a group is unique, $(G, \circlearrowleft)$ and $(H, \circlearrowleft)$ must contain the same identity element, which is $e_G$. Therefore $(H, \circlearrowleft)$ contains $e_G$.

- For every group, the set containing just the identity element (of a group) is a subgroup (of that group). This is because identity element is contained in the group (otherwise the group properties would not be satisfied for this group). It has an identity by definition, it is its own inverse and is closed under the group operation by definition. The subgroup containing just the identity element is called a trivial subgroup.

Cosets

The coset of a subgroup (along with an element of the group) is the set containing the results of the binary operation between the given element and every element of the subgroup. Since the group in general is non-Abelian, we see that if $(H, \circlearrowleft)$ is a subgroup of $(G, \circlearrowleft)$ then for some $g \in (G, \circlearrowleft)$ and $h \in (H, \circlearrowleft)$, $g \circlearrowleft h$ need not be equal to $h \circlearrowleft g$. Therefore we need to specify which ‘sided’ a particular binary operation is. Hence have ‘left’ and ‘right’ cosets.

**Left and Right Cosets**:
- **Left Coset**: $g \circlearrowleft (H, \circlearrowleft) = \{g \circlearrowleft h | h \in (H, \circlearrowleft)\}$ (3.27)
- **Right Coset**: $(H, \circlearrowleft) \circlearrowleft g = \{h \circlearrowleft g | h \in (H, \circlearrowleft)\}$ (3.28)

We can now look at a few properties of cosets.

1. From the definitions in (eq. 3.27) and (eq. 3.28), the number of elements in the left and right cosets of a subgroup in a group is equal to the order of the subgroup.

2. **Assumption**: $g \circlearrowleft (H, \circlearrowleft) = (H, \circlearrowleft) \circlearrowleft g = (H, \circlearrowleft)$ $\forall g \in (H, \circlearrowleft)$.

   **Justification**: Since $(H, \circlearrowleft)$ forms a group it is closed under the $\circlearrowleft$ operation. Hence from (eq. 3.27) we see that $\forall g, h \in (H, \circlearrowleft)$ $g \circlearrowleft h \in (H, \circlearrowleft)$, and similarly from (eq. 3.28) we have $\forall g, h \in (H, \circlearrowleft)$
h ⊕ g ∈ (H, ⊕). Hence we see that all the elements in g ⊕ (H, ⊕) and (H, ⊕) ⊕ g are in (H, ⊕), ∀g ∈ (H, ⊕). Hence we have the justification.

3. Assumption: ∀g ∈ (G, ⊕), the identity element of (G, ⊕): e_G is contained in g ⊕ (H, ⊕) and (H, ⊕) ⊕ g. Justification: It suffices to show that ∃g ∈ (G, ⊕) such that e_G = g ⊕ h and e_G = h ⊕ g. This is true as both (G, ⊕) and (H, ⊕) contain e_G, so setting g = h = e_G, we provide the justification.

4. Assumption: Every element of (G, ⊕) is present in exactly one of the left cosets of (H, ⊕) in (G, ⊕). Justification: If an element is present in two different left cosets, say g_1 ⊕ (H, ⊕) and g_2 ⊕ (H, ⊕), of (H, ⊕) in (G, ⊕) then ∃g_1, g_2, h ∈ (G, ⊕) with g_1 ≠ g_2 such that g_1h = g_2h. From (eq. 1) of (sec. 3.1.1) we see that if g_1 ≠ g_2, then g_1h ≠ g_2h. Also note that g_1h = g_2h implies that g_1 = g_2, which means that the two left cosets are identical. Hence we have the justification.

5. Assumption: Every pair of cosets (of (H, ⊕) in (G, ⊕)) are either disjoint or identical. Justification: In the previous statement we have showed that no two left cosets can share the same element unless the left cosets are identical, implying that every pair of left cosets is disjoint, unless they are alike. Hence we have the justification.

6. Assumption: ∃ no g ∈ (G, ⊕) which is not present in any left coset of (H, ⊕) in (G, ⊕). Assumption: Consider the coset g ⊕ (H, ⊕). It suffices to show that g ∈ g ⊕ (H, ⊕) ∀g ∈ (G, ⊕). For g ∈ (H, ⊕) this statement is trivially true. Else, it means that ∃h ∈ (H, ⊕) such that g = g ⊕ h. As (H, ⊕) contains the identity element e_G, we see that the previous statement is true, thereby justifying the assumption.

7. From the assumptions in (statement. 5) and (statement. 6), we see that the cosets of a subgroup in a group, are all disjoint and they cover all the elements of the group. In other words, they partition the group, with each partition being a coset. Notice that # elements in (G, ⊕) = [(G, ⊕)]. From (statement. 1) we have that # elements in a left coset = [(H, ⊕)]. Hence we see that # left cosets needed to partition (G, ⊕) = [(G, ⊕)] / [(H, ⊕)]. This quantity is denoted by [(G, ⊕) : (H, ⊕)] and called the index of (H, ⊕). The theorem named after this equation is called Lagrange’s Theorem.

Index of a Subgroup: The index of a subgroup of a group is the number of left cosets of the subgroup required to partition the group.

\[
[(G, ⊕) : (H, ⊕)] = \frac{|(G, ⊕)|}{|(H, ⊕)|}
\] (3.29)

Normal Subgroup: A normal subgroup (N, ⊕) of a group (G, ⊕) is such that the right and left cosets of x in (N, ⊕) are equal ∀(G, ⊕).

Normal Subgroup (N, ⊕) of (G, ⊕): \(a ⊕ N = N ⊕ a \ \forall a ∈ (G, ⊕)\) (3.30)

3.1.3 Quotient Groups

We see clearly that the coset does not form a group. So we consider the set of all cosets of a normal subgroup (left or right, it does not matter). Let (N, ⊕) be a normal subgroup of (G, ⊕). Consider the set \(S = \{a ⊕ N|a ∈ (G, ⊕)\}\). We claim this set forms a group. To check we have:

- Identity, Inverse and Associativity are trivially satisfied as the one of the cosets contain the identity and as (G, ⊕) is a group, the elements in it have their associated inverses.
- Closure: We need to show that: \((a ⊕ N) ⊕ (b ⊕ N) ∈ S \ ∀(a ⊕ N), (b ⊕ N) ∈ S\).
  For this it suffices to show that \((a ⊕ N) ⊕ (b ⊕ N) = (c ⊕ N)\) for some \(c ∈ (G, ⊕)\). Now notice that:

\[
(aN) ⊕ (bN) = a ⊕ ((Nb) ⊕ N)
\]

normal subgroups coset = \((a ⊕ b) ⊕ (N ⊕ N)\)

\[= (a ⊕ b) N\]
Now since \( a, b \in (G, \circ) \) we have: \( (a \circ b) \in (G, \circ) \), thereby justifying the assumption.

Hence we see that \( S \) forms a group under the \( \circ \) operation. This group formed by the elements of \( S \) is called the quotient group of \((G, \circ)\) and is represented as: \((G, \circ) / (N, \circ)\).

**Quotient Group:** The quotient group of \((G, \circ)\) is the set \( \{g \circ N | g \in (G, \circ)\} \) containing all the cosets (right or left) of its elements in of its normal subgroup. It is represented as \((G, \circ)\).

More generally, since the cosets of elements in a subgroup partition the group, the quotient group is the group formed by the partition of \((G, \circ)\) along with the operation \( \circ \) defined analogously.

### 3.1.4 Normalizers and centralizers

For any two elements \( A, B \) of a group: \((G, \circ)\), we note that unless the group is Abelian, the result of the binary operation \( \circ \) of the two elements depends upon the order in which they are considered: \( A \circ B \neq B \circ A \).

**Commutator:** The commutator for any two elements \( A \) and \( B \) of a group \((G, \circ)\) is defined as: \( [A, B] = A \circ B - B \circ A \).

From the definition of the commutator we can verify that \( \forall g_1, g_2 \in (G, \circ): [g_1, g_2] = 0 \) and \( [g_1, g_2] = -[g_2, g_1] \).

Based on this commutator we have the following sets associated with the group elements:

**Center of a group:** The center of a group \( Z(G, \circ) \) is the set of all elements in \((G, \circ)\) that commute with all the elements in \((G, \circ)\). Hence \( Z(G, \circ) = \{g \in (G, \circ) | g \circ x = x \circ g | x \in (G, \circ)\} \).

Since in an Abelian group, all the elements commute with each other, we see that the centre of an abelian group is the group itself, i.e., \( Z(G, \circ) = (G, \circ) \) \( \forall \) Abelian groups \((G, \circ)\).

For any subgroup (of a group) we define the following two groups:

**Normalizer:** The normalizer of a subgroup \((H, \circ)\) of \((G, \circ)\) is the set:

\[
\mathcal{N}(H, \circ) = \{g | (g \circ h_1) \circ g^{-1} \in (H, \circ) \ \forall g \in (G, \circ)\} \tag{3.31}
\]

**Centralizer:** The centralizer of a subgroup \((H, \circ)\) of \((G, \circ)\) is the set:

\[
Z(H, \circ) = \{g | (g \circ h_1) \circ g^{-1} = h_1 \ \forall g \in (G, \circ)\} \tag{3.32}
\]

We can now look at some properties of the centralizers and the normalizers of a subgroup.

1. Immediately one can see that the elements in \( Z(H, \circ) \) form a subset of those in \( \mathcal{N}(H, \circ) \).

2. The centralizer of a subgroup forms a subgroup (of a group) of the underlying group, i.e., \( Z(H, \circ) \) and \((H, \circ)\) are subgroups of \((G, \circ)\).

**Justification:** Notice that the definition of the centralizer can also be given as the set of elements of the subgroup that commute with each element in the group. \( Z(H, \circ) = \{g | g \circ h = h \circ g, \forall g \in (H, \circ)\} \).

With this denition we can verify the group properties of \( Z(H, \circ) \).

- **Identity:** Trivially identity commutes with all the elements of the group and hence it is in \( Z(H, \circ) \).

- **Inverse:** If \( x \in Z(H, \circ) \) then \( x^{-1} \in Z(H, \circ) \).

**Justification:** We see that \( x \circ y = y \circ x, \forall y \in Z(H, \circ) \). Notice that if it suffices to show:

\[
\begin{align*}
x^{-1} \circ y &= y \circ x^{-1} \forall y \in (G, \circ) \\
x \circ y &= y \circ x \forall x \in (G, \circ)
\end{align*}
\]

Since \( x \in (G, \circ) \) which is a group, \( \exists x^{-1} \in (G, \circ) \) such that \( x \circ x^{-1} = e_G \).

\[
x \circ y = y \circ x \tag{3.33}
\]

\[
\begin{align*}
(x^{-1} \circ (x \circ y) \circ x^{-1}) &= (x^{-1} \circ (y \circ x) \circ x^{-1}) \\
(x^{-1} \circ x) \circ (y \circ x^{-1}) &= (x^{-1} \circ y) \circ (x \circ x^{-1}) \\
y \circ x^{-1} &= x^{-1} \circ y
\end{align*}
\]

Hence justifying the assumption.

- **Closure:** \( a \circ x \in Z(H, \circ) \ \forall x, a \in Z(H, \circ) \)

**Justification:** It suffices to show that \( (a \circ x) \circ y = y \circ (a \circ x) \). Notice that since \( x, y \) and \( a \) are...
elements of \( Z \langle H, \circ \rangle \), they commute with all elements in \( (G, \oplus) \).

\[
(a \circ x) \circ y = a \circ (y \circ x) = y \circ (a \circ x)
\]

Hence justifying the theorem.

Hence from the above statements it can be seen that \( Z \langle H, \circ \rangle \) is group, moreover it is a subgroup of \( (G, \oplus) \).

Note that the center of a group is not to be confused with the centralizer of a subgroup in a group. The former is the set of elements in \( (G, \oplus) \) which commute with every element in \( (G, \oplus) \), while the latter is the set of all elements in \( (G, \oplus) \) that commute with every element in the subgroup \( (H, \circ) \). Hence the latter is defined with respect to a subgroup unlike the former. However, both the center (of a group) as well as the centralizer (of any subgroup in that group) are subgroups of the underlying group.

### 3.2 Group Operations

#### 3.2.1 Direct product of groups

**Direct product:** The direct product of two groups \( (H, \circ) \) and \( (K, \oplus) \), represented by \( (H, \circ) \times (K, \oplus) \) is a group containing \( (h, k), \forall h \in (H, \circ), k \in (K, \oplus) \).

We can define the group operations on \( (H, \circ) \times (K, \oplus) \) are:

\[
(h_1, k_1) \circ (h_2, k_2) = (h_1 \circ h_2, k_1 \oplus k_2)
\]

The identity element of this direct product group is the tuple containing the identity elements of the individual groups: \((e_H, e_K)\). The inverse of an element is also the tuple containing the inverse of the corresponding elements from the two groups (in the product).

#### 3.2.2 Homomorphism

**Homomorphism:** For any two groups \( (G, \oplus) \) and \( (H, \circ) \), a group homomorphism is a function \( f : (G, \oplus) \rightarrow (H, \circ) \) whose action on the elements of \( a, b \in G \) is given by:

\[
f (a \oplus b) = f (a) \circ f (b)
\]

Notice that it preserves the group structure, i.e., if the elements in \( G \) form a group, so do the elements in the set \( H \). We can now see some properties of \( f \). Let \( e_G \) and \( e_H \) denote the identity elements of the groups \( (G, \oplus) \) and \( (H, \circ) \) respectively.

Using (eq. 3.34):

\[
f (a \oplus e_G) = f (a) \circ f (e_G)
\]

\[
f (a) = f (a) \circ f (e_G)
\]

\[
(f(a))^{-1} \circ f (a) = (f(a))^{-1} \circ (f (a) \circ f (e_G))
\]

\[
e_H = (f(a))^{-1} \circ f (a) \circ f (e_G)
\]

\[
e_H = f (e_G)
\]

Hence we see that the identity element of \( (G, \oplus) \) is mapped to the identity element of \( (H, \circ) \). We now see the mapping of the inverse of an element in \( (G, \oplus) \). From (eq. 3.34), for \( u \in (G, \oplus) \):

\[
f (u) \circ f (u^{-1}) = f (e_G)
\]

Using (eq. 3.35):

\[
[f (u)]^{-1} \circ f (u) \circ f (u^{-1}) = [f (u)]^{-1} \circ e_H
\]

\[
\therefore f (u^{-1}) = [f (u)]^{-1}
\]
Hence we see that $f$ maps the inverse of every element to the inverse of its image in $(H, \odot)$.

**Types of Homomorphisms**

**Isomorphism:** It is a homomorphism $f : (G, \odot) \rightarrow (H, \odot)$, where $f$ is one-to-one. Hence $f^{-1}$ too is a homomorphism.

**Automorphism:** It is an isomorphism from a group onto itself: $f : (G, \odot) \rightarrow (G, \odot)$.

**Endomorphism:** It is a homomorphism from a group onto itself: $f : (G, \odot) \rightarrow (G, \odot)$. Note: $f$ is not one-to-one.

**Kernel**

We now consider the elements in $(G, \odot)$ that are mapped to the same element in $(H, \odot)$ by the homomorphism. As the identity element $e_H$ is unique to $(H, \odot)$, the properties of this element can be referred to as the properties of the group. Hence, we consider all the elements in $(G, \odot)$ that are mapped to $e_H$. The set containing all such elements is called the kernel of $f$, denoted as $\ker(f)$.

$$\ker(f) = \{ g \in (G, +_q) \mid f(g) = e_H \}$$

(3.37)

The kernel is useful in associating a homomorphism to a set. That is we can check the containment of an element in a set by checking the action of the corresponding homomorphism (associated with that set) on the element in question. When we talk of $(G, \odot)$ and $(H, \odot)$ being linear codes, or vector spaces over the field $\mathbb{F}_q$ we see that $\odot$ becomes addition modulo $q$, $+_q$. Notice that the identity element here is the null vector. So the kernel of the homomorphism (in this case it is a linear map represented by a matrix) is the set of vectors in $(G, +_q)$ that are mapped to the null vector in $(H, +_q)$. We now pick a linear map such that the kernel of this linear map is the linear code. The advantage of doing this is that we can quickly identify a code element by checking if it gives the null vector upon action of this linear map. Such a linear map (represented by a matrix) is called the Parity Check Matrix of the linear code. It is used to check for errors in the codewords. If there is an error in the codeword, the vector undergoes a translation such that the new vector no more belongs to the vector space, and hence does not lie in the kernel or the parity check matrix. Therefore upon action of this matrix it will not give the null vector, thereby indicating the presence of an error.

### 3.2.3 Conjugation

Two elements of a group $a, b \in (G, \odot)$ are said to be conjugate to each other if $\exists g \in (G, \odot)$ such that: $g \odot a = b \odot g$. Restating the previous statement, we have: $b$ is conjugate to $a$ if $\exists g \in (G, \odot)$ such that $b = (g \odot a) \odot g^{-1}$. We can further formalize this by looking at the RHS of previous equation as a function of $a$: $b = f(a)$, where $f(a) = (g \odot a) \odot g^{-1}$. This function, or automorphism (as it takes an element in $(G, \odot)$ to itself) is called inner automorphism or conjugation.

**Conjugation or Inner-Automorphism:** It is an automorphism defined by $f : (G, \odot) \rightarrow (G, \odot)$ such that for some $a, g \in (G, \odot)$, $f(a) = g \odot (a \odot g^{-1})$.

We now consider the set of all elements (in a group) that are conjugate to a given element (from the same group). That is the set $\{ b \mid g \odot a = b \odot g, \quad g \in (G, \odot) \}$. Note that since $a$ is the free variable in the definition of this set, it must be indexed by $a$. We can also write this set as: $S_a = \{ g \odot (a \odot g^{-1}) \mid g \in (G, \odot) \}$. Such a set is called the conjugacy class of $a$.

**Conjugacy Class:** Conjugacy class of an element (in a group) is the set containing all the elements from that group which are conjugate to the given element.

$$Cl(a) = \{ g \odot (a \odot g^{-1}) \mid g \in (G, \odot) \}$$

(3.38)

We can now look at some properties of this set:

---

2Note that, from (eq. 3.35), $e_G$ is one of them.
1. Assumption: If \( g \) is an element of an Abelian group, \( \forall g \in (G, \circ), \ #\text{Cl}(a) = 1 \), that is \( \text{Cl}(a) \) is a singleton set.

Justification: To see this, we try to write the definitions of the abelian group, and the conjugacy class of an element, in the same form.

\[
\text{Cl}(a) = \{b|g \circ a = b \circ g, \ g \in (G, \circ)\}
\]

\[
G = \{b|g \circ b = b \circ g, \ g \in (G, \circ)\}
\]

Notice that the conjugacy class of an element from an Abelian group has to satisfy the conditions in the above definitions, we see that the only 'solution', or satisfying assignment for \( a \) (it is the only free variable) is \( a = b \). Hence we see that: \( \text{Cl}(a) = \{b|g \circ a = b \circ g, a = b, \ g \in (G, \circ)\} \Rightarrow \{a\} \).

Hence we justify our assumption.

### 3.3 Group Actions

#### 3.3.1 Generating set of a group

As the elements of a group satisfy certain properties, given a set \( X \) it must be possible to construct (or mechanically generate from this set) a subset following these properties. In otherwords, we can take a set of elements and then generate a group such that group properties are satisfied by construction. Such a set is called a generating set of a group and the elements of this set are called generators.

**Generating Set of a Group:** A generating set of a group \((G, \circ)\) is a set \( X \) such that every element of \((G, \circ)\) can be expressed as a combination (using \( \circ \)) of finite subset of \( X \). We denote it by: \((G, \circ) \equiv \langle X \rangle\).

Since a group is also a set of elements, it can also be used to generate another group. More generally we can use more than one group to generate a single group. That is elements in groups \((H, \circ), (G, \circ)\) can be used to generate the elements of \((G, \circ)\). In this case we say that \((G, \circ)\) is a direct sum of subgroups \((H, \circ)\) and \((K, \circ)\). But for this to be possible notice that \((H, \circ)\) has to be a normal subgroup of \((G, \circ)\).

**Direct sum of Groups:** A group \((G, \circ)\) is a direct sum of groups \((H, \circ)\) and \((K, \circ)\), represented as \((G, \circ) = (H, \circ) \oplus (K, \circ)\) if the generating set of \((G, \circ)\) \( \subseteq H \cup K \), and \((H, \circ)\) and \((K, \circ)\) are normal subgroups of \((H, \circ)\).

#### 3.3.2 Symmetric group

We now try to explore the properties of a given set \( X \) using groups. By exploring the properties, we mean to look at all possible relations between the elements of the set. For this we need to consider the set of all functions \( \{h : X \to X\} \), since each function relates one element of \( X \) with another. For the sake of simplicity, we avoid relations between a given element and many other elements. Hence we only consider all possible one-to-one functions (or bijections). This set containing all possible bijections from \( X \) to \( X \) also forms a group under the composition (of two functions) operation.

**Symmetric Group:** A symmetric subgroup on a set \( X \) is a group formed by the set \( G \) containing all possible bijections \( f : X \to X \), under the binary operation \( \circ \) which denoted the composition of two functions. This group \((G, \circ)\) satisfies the group properties.

We can now verify the group properties of this symmetric group:

- **Closure:** \( \forall f, g \in (G, \circ), \ (f \circ g) \in (G, \circ) \).
  
  For this it suffices to show that \( f \circ g \) is also a bijection. Notice that \( \forall x \in X, \ (f \circ g)(x) = f(g(x)) \).

  Since \( g \) is a bijection \( g : X \to X \) we see that \( g(x) \) is injective and surjective \( [g(X) = (X)] \). Hence all values of \( g(x) \) are distinct \( (\forall \text{ distinct } x \in X) \). As \( f \) is again a bijection from \( X \) to \( X \), it will take each of these distinct \( g(x) \) (corresponding to distinct \( x \)) to some \( f(x) \in X \). Therefore all values of \( f(x) \) are distinct \( (\forall \text{ distinct } x \in X) \). Hence \( f \circ g \) is injective. As \( f(X) = X \), we see that \( f(g(X)) = X \). Hence \( f \circ g \) is both surjective and injective, thereby bijective, hence justifying the assumption.
3.3. GROUP ACTIONS

- Associative: \( \forall \alpha, \beta, \gamma \in (G, \circ), \alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma \).
  The above statement is true as we have: \( [\alpha \circ (\beta \circ \gamma)] x = [(\alpha \circ \beta) \circ \gamma] x = \alpha (\beta (\gamma(x))) \) \( \forall x \in X \). This is in general true for any three functions. Hence we justify the assumption.

- Identity: \( \exists e_G \in (G, \circ) \) such that \( \forall f \in (G, \circ), e_G \circ f = f \circ e_G = f \).
  It suffices to show that there is a bijection \( e_G \) such that \( \forall f \in (G, \circ) \) and \( \forall x \in X \), we have: \( f(e_G(x)) = e_G(f(x)) = f(x) \). We can now see that \( e_G \) is nothing but the identity map: \( e_G \equiv \mathcal{I}_X \), which clearly is a bijection and hence \( \in (G, \circ) \). Hence we justify the assumption.

- Inverse: \( \forall f \in (G, \circ) \) \( \exists g \in (G, \circ) \) such that \( f \circ g = g \circ f = e_G \).
  It suffices to show that \( \forall f \in (G, \circ) \) \( \exists g \in (G, \circ) \) such that \( \forall x \in X \) we have: \( f(g(x)) = g(f(x)) = x \).
  We can now see that \( g \) is nothing but the inverse map: \( f^{-1} \), which clearly is a bijection since \( f \) is a bijection. Hence we see that there is an inverse in \( (G, \circ) \) for every element in it, thereby justifying the assumption.

3.3.3 Action of Group on a set

In the above section (sec. 3.3.2) we considered a group of bijections on a set \( X \). Now we consider a general group \( (Q, \oplus) \) and a homomorphism: \( h \) from \((Q, \oplus)\) to the symmetric group of \( X \): \( (G, \circ) \). Every element of \((Q, \oplus)\) is mapped to a bijection on \( X \). As a result we can describe the action of the bijection (on some \( x \in X \)) as the action of the element of \((Q, \oplus)\) (which has been mapped to this bijection by the homomorphism \( h \)).

Therefore the homomorphism is defined as: \( h : (Q, \oplus) \rightarrow (G, \circ) \) such that:

\[
\forall q_1, q_2 \in (Q, \oplus), \quad h(q_1 \oplus q_2) = h(q_1) \circ h(q_2)
\]

(3.39)

Note that \( h(q) \) is a bijection \( \forall q \in (Q, \oplus) \), that is in the above expression: \( h(q_1) : X \rightarrow X \). The homomorphism maps the identity of \((Q, \oplus)\) to identity element of \((G, \circ)\) the inverse of every element in \((Q, \oplus)\) is mapped to the inverse of the corresponding element’s map.

\[
h(e_Q) = \mathcal{I}_X
\]

\[
\forall q \in (Q, \oplus), \quad h(q^{-1}) = (h(q))^{-1}
\]

Now when we want to describe the operation \([h(q_1)](x)\) for \( x \in X \), we denote it as action of \( q_1 \) on \( x \): \( q_1 \cdot x \). Similarly \([(h(q))(x)]q \in (Q, \oplus))\) can be denoted as: \( \{q \cdot x|q \in (Q, \oplus)\} \) and hence \( Q \cdot X = \{q \cdot x|x \in X, q \in (Q, \oplus)\} \). This operation is called action of a group on a set, or group action. The group action can be described as a function that takes an element of \((Q, \oplus)\) and an element of \( X \), giving another element of \( X \). Hence the group action on a set is described as another homomorphism from \((Q, \oplus) \times X \to X \).

**Group Action**: The Group Action of \((Q, \oplus)\) on a set \( X \) is defined as a homomorphism: \( f : (Q, \oplus) \times X \rightarrow X \) such that: for \( x \in X, q \in (Q, \oplus) \) we have: \( f(q, x) = q \cdot x \) which represents \( q \cdot x \equiv [h(q)](x) \) where \( h \) is as defined in (eq. 3.39).

3.3.4 Orbits and Stabilizers

We now need to look at the geometric picture by considering \( X \) to be a set of points (in \( \mathbb{R}, \mathbb{C} \), or anything,) and the action of elements \( q \in (Q, \oplus) \) (which is the action of \( h(q) \) as defined in (eq. 3.39)). When \( q \cdot x = x' \) where \( x' \in X \) we say that \( x \) has been transported to the point \( x' \) and the path taken by \( x \) is the set \( \{x, x'\} \).

Consider the set \((Q, \oplus) \cdot x = \{q \cdot x|q \in (Q, \oplus)\}\). This says all the points which can be obtained by acting the elements of \((Q, \oplus)\) on \( x \). In other words it gives the path traced by the point \( x \in X \) upon action of elements in \((Q, \oplus)\). This path represented by the set of points is called the **Orbit** of \( x \), denoted by \( D_{(Q, \oplus)}(x) \).

\[
\text{Orbit} : \text{Orbit of an element } x \in X : \quad D_{(Q, \oplus)}(x) = (Q, \oplus) \cdot x \equiv \{q \cdot x|q \in (Q, \oplus)\}
\]

(3.40)

Since \( x \) is a finite set, it may happen that the path traced by \( x \) contains \( x \) itself. Suppose the path taken by \( x \) has points \( \{x, x_1, x_2, \ldots x_m, x \ldots x_n, x \ldots x_k, x \ldots \} \) we have:

**GO TO FIRST PAGE**
\[ x \xrightarrow{q_1} x_1 \quad x_1 \xrightarrow{q_2 \cdots q_{m-1}} x_m \quad x_m \xrightarrow{q_m} x_{m+1} \quad x_{m+1} \xrightarrow{q_{m+1} \cdots q_{k-1}} x_k \xrightarrow{\ldots} \] which can now be rewritten as:
\[ x \xrightarrow{q_1} x_1 \quad x_1 \xrightarrow{q_2} x_2 \quad \ldots \quad x_{m-1} \xrightarrow{q_{m-1}} x_m \quad x_m \xrightarrow{q_m} x_{m+1} \quad \ldots \]
We now see that the set of operators: \( S_x(Q, \circ) = \{ q_1 \circ q_2 \circ \cdots \circ q_{m-1} \circ q_m \circ q_{m+1} \circ \cdots \circ q_{k-1} \circ q_k \} \) leave the point \( x \) invariant. Now since \( q_1, q_2, \ldots, q_m, \ldots, q_n \in (Q, \circ) \), we see that the operators in \( S_x(Q, \circ) \) are also in \((Q, \circ)\). Moreover, the identity operator \( e_Q \in S_x(Q, \circ) \) (since it corresponds to the identity mapping) and since each of these operators correspond to a bijection (on \( X \)), an inverse can be defined easily which also is a bijection that leaves \( x \) invariant. Hence \( S_x(Q, \circ) \) contains the inverse of element in it. Note that the set \( S_x(Q, \circ) \) is closed under \( \circ \), has an identity element and every element in this set has its inverse in the same set. Therefore the set \( S_x(Q, \circ) \) along with the operation \( \circ \) forms a group, and trivially a subgroup of \((Q, \circ)\). This subgroup is called the \textbf{Stabilizer Subgroup} of \((Q, \circ)\).

**Stabilizer Subgroup:** The stabilizer subgroup \( S_x(Q, \circ) \) (of a group) consists of elements that leave an element \( x \in X \) invariant.

\[ S_x(Q, \circ) = \{ q \in (Q, \circ) \mid q \cdot x = x \} \quad (3.41) \]

### 3.3.5 Orbit Stabilizer theorem

We now have a theorem similar to lagrange’s theorem in (eq. 3.29), relating the sizes of \( D(x) \), \( S_x(Q, \circ) \) and \((Q, \circ)\).

**Theorem:** For any group, the number of elements in the orbit, with respect to any element in the set and the stabilizer subgroup (of this group) with respect to the same element of the set are related by:

\[ |D(x)| \times |S_x(Q, \circ)| = |(Q, \circ)| \quad (3.42) \]

**Proof:** Let us denote \( S_x(Q, \circ) \equiv S(x) \). Consider the slight modification of \( S(x) \) (eq. 3.41) as:

\[ S_y(x) = \{ q \in (Q, \circ) \mid q \cdot x = y \} \quad (3.43) \]

\[ S_x(x) = S(x) \quad (3.44) \]

We now claim that the sets \( S_y(x) \) for different \( y \) are disjoint.

\[ \forall y_1, y_2 \in X, y_1 \neq y_2 \text{ the sets } S_{y_1}(x) \text{ and } S_{y_2}(x) \text{ are disjoint.} \]

**Justification:** It suffices to show that if \( \exists q \in S_{y_1} \cap S_{y_2} \), then \( y_1 = y_2 \). This is true since in the former case we will have: \( q \cdot x = y_1 \) and \( q \cdot x = y_2 \), which clearly implies \( y_1 = y_2 \), thereby justifying the assumption.

We now have: \((Q, \circ) = \bigcup_{y \in D(x)} S_y(x)\) and hence:

\[ |(Q, \circ)| = \sum_{y \in D(x)} |S_y(x)| \quad (3.45) \]

We now claim that each set \( S_y(x) \) for every value of \( y \in X \) has the same cardinality which can be equated to that of \#\( S_x(x) \) which is, from (eq. 3.44): |\( S(x) |\).

**Assumption:** For every \( y \in X \), \#\( S_y(x) = |S| \).

**Justification:** It suffices to show that \( \exists \) a bijection \( f : S \rightarrow S_y(x) \), \( \forall y \in X \). We now try to construct this bijection. For a fixed \( t \in S_y(x) \) and \( \forall h \in S \) define the bijection as: \( f(h) = t \circ h \). Notice that \( (t \circ h) \cdot x = t \cdot (h \cdot x) \) which from (eq. 3.41) \( = t \cdot x \Rightarrow y \) using (eq. 3.43). To show that \( f \) is a bijection, we need to show that \( f \) is injective and surjective.

**Injective:** For \( f(h_1) = f(h_2) \), then \( t \cdot h_1 = t \cdot h_2 \) which implies \( h_1 = h_2 \). So if \( h_1 \neq h_2 \) then \( f(h_1) \neq f(h_2) \).

**Surjective:** We need to show that every element in \( S_y(x) \) is covered in the image of \( f \), for some \( x \in X \). It suffices to show that every element in \( S_y(x) \) can be represented in the form of the image of \( f \). Equivalently
we can show that $\forall u \in \mathfrak{H}_y(x), \exists t \in \mathfrak{H}_y(x)$ such that $t^{-1} \cdot u \in \mathfrak{G}$.

From (eq. 3.43): $u \cdot x = y \quad \& \quad t \cdot x = y$  \hspace{1cm} (3.46)

$\therefore \quad x = t^{-1} \cdot y$

Using (eq. 3.46): $u \cdot x = t^{-1} \cdot (u \cdot x)$

$\therefore \quad x = (t^{-1} \cdot u) \cdot x$

Now from (eq. 3.41) we have: $(t^{-1} \cdot u) \in \mathfrak{G}(x)$. Hence we have the justification.

Now we see that $f$ is a bijection and $\forall y \in X, \# \mathfrak{H}_y(x) = |\mathfrak{G}|$. In (eq. 3.45) we can replace the sum by a product as all the entities being summer over have the same value. We then have the statement as in the theorem (eq. 3.42). Hence we have proved the theorem.