PROPERTIES OF COMMUTATORS

APPROVED:

N. A. Vaughan
Major Professor

George Copp
Minor Professor

A. C. Parrish
Director of the Department of Mathematics

Robert B. Toulouse
Dean of the Graduate School
PROPERTIES OF COMMUTATORS

THESIS

Presented to the Graduate Council of the
North Texas State College in Partial
Fulfillment of the Requirements

For the Degree of

MASTER OF SCIENCE

By

Merle Dean Roach, B. S.

Denton, Texas
August, 1959
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Chapter</th>
<th></th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I.</td>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Assumptions and Definitions</td>
<td></td>
</tr>
<tr>
<td>II.</td>
<td>FUNDAMENTAL LEMMAS</td>
<td>7</td>
</tr>
<tr>
<td>III.</td>
<td>BASIC THEOREMS ON COMMUTATORS</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>BIBLIOGRAPHY</td>
<td>21</td>
</tr>
</tbody>
</table>
CHAPTER I

INTRODUCTION

A mathematical system consists of elements denoted by \( a, b, c, \ldots \); an equals relation, \( = \); certain operations; and a set of postulates which the elements and operations satisfy. The equals relation serves to separate the elements into classes; two elements being equal if and only if they belong to the same class.\(^1\)

An equals relations, \( a = b \), is characterized by the following four postulates:

(1) Either \( a = b \), or \( a \neq b \).\(^2\) (The relation is determinative.)

(2) \( a = a \). (The relation is reflexive.)

(3) If \( a = b \), then \( b = a \). (The relation is symmetric.)

(4) If \( a = b \) and \( b = c \), then \( a = c \). (The relation is transitive.)

An operation relates to every ordered pair of elements \( a, b \), a third element \( c \); i.e., given a first element \( a \) and a second element \( b \), the operation defines a third element \( c \).


\(^2\)\( a \neq b \) means "a not equal to b."
If the symbol $X$ is used as the symbol of the operation, this relation may be written

$$a \ X \ b = c.$$ 

For simplification, $a \ X \ b$, will be abbreviated to $ab$. The operation is well defined, relative to the equals relation, if, when $a$, $b$, or both $a$ and $b$ are replaced by equal elements, $c$ is also replaced by an equal element.

One of the simplest mathematical systems of consequence is the group. It is composed of elements, an equals relations, and one operation. The symbol $X$ will denote the operation, which will be called abstract multiplication. (For elements $a$, $b$, of a group, $ab$ will mean $a \ X \ b$.) The group operation is subject to the following four postulates:

1. The system is closed under the operation, which is well defined. That is, if $a$ and $b$ are elements of a group, then $c = ab$ is an element of the group.

2. The operation is associative. That is, for elements $a$, $b$, and $c$ of a group,

$$ (ab)c = a(bc).$$

3. There exists an identity element $I$, such that,

\begin{itemize}
\item[$^4$] $(x)(y)$ means $x \ X \ y$.
\end{itemize}
al = la = a

for every element of the group.

(4) Every element a has an inverse, denoted by a', such that

a'a = aa' = 1.

If the elements of a group commute, i.e., if

ab = ba,

the group is called a commutative group or an abelian group.5

A finite group is a group consisting of a finite number of elements. The number of elements in a finite group is the order of the group.

This paper deals exclusively with finite groups; however, many of the properties of finite groups and theorems considered apply to infinite groups. Reference to an arbitrary group G will imply reference to a finite group.

If a and b are elements of a group G, the element

[a, b] = aba'b' is called the commutator of a and b.6 The formation of the commutator is regarded as a new operation defined on the set of group elements.

This paper is a study of the properties of commutators.

---


6Ibid., p. 78.
Assumptions and Definitions

The following fundamental theorems and definitions will be assumed.

**Theorem 1.1.** The product of $k$ elements of a group is independent of the manner in which the elements are associated. That is,

\[(a_1 a_2 \cdots a_{k-1} a_k) = a_1 (a_2 \cdots a_{k-1} a_k) = (a_1 a_2 \cdots a_{k-1}) a_k.\]

**Definition 1.1.** $a^n = a a \cdots a$, ($n$ factors $a$).

**Theorem 1.2.** The identity element $1$ is unique.

**Theorem 1.3.** If $ab = ac$, then $b = c$.

**Corollary 1.31.** The inverse of an element is unique.

**Corollary 1.32.** The equation $ax = b$ has a unique solution.

**Theorem 1.4.** $(a')' = a$.

**Theorem 1.5.** The inverse of a product is the product of the inverses taken in reverse order, i.e.,

\[(ab)' = b'a'.\]

**Definition 1.2.** $a^{-m} = (a')^m = (a^m)'$.

**Theorem 1.6.** If $m$ and $n$ are integers,

\[a^m a^n = a^{m+n}.\]

**Theorem 1.7.** If $m$ and $n$ are integers,

\[(a^m)^n = a^{mn}.\]

**Theorem 1.8.** If $n$ is an integer and if $a$ and $b$ commute, then

\[a^n b^n = (ab)^n.\]
Definition 1.3. A subset \( K \) of a group \( G \) is called a subgroup if the elements of \( K \) form a group relative to the operation defined for \( G \).

Definition 1.4. A subgroup \( K \) of a group \( G \) is called a proper subgroup if \( K \) is not \( G \).

Definition 1.5. The symbol \( \in \) shall mean "is an element of" or "are elements of."

Definition 1.6. The symbol \( \subseteq \) shall mean "is contained in" or "is a subset of."

Definition 1.7. A left coset of a subgroup \( H \), contained in a group \( G \), is defined to be the set, \( Hx \), consisting of elements of the form \( hx \), where \( h \) ranges over the set \( H \) and \( x \) is a fixed element of \( G \). Similarly, a right coset of a subgroup \( H \), contained in a group \( G \), is defined to be the set, \( xH \), consisting of elements of the form \( xh \), where \( h \) ranges over the set \( H \) and \( x \) is a fixed element of \( G \).

Definition 1.8. A subgroup \( S \) which separates a group \( G \) into the same cosets by right multiplication as by left multiplication is called an invariant subgroup of \( G \). An invariant subgroup is also called normal or self-conjugate.\(^8\)

\(^7\)Ibid., p. 10.
\(^8\)Ibid., p. 46.
It should be noted that invariance is a "set operation", not an "element operation."

**Theorem 1.2.** Consider a group $G$. The set $C$, consisting of all elements of $G$ which commute with every element of $G$, forms a subgroup of $G$.

**Definition 1.9.** The set $C$ described in Theorem 1.9 shall be called the center of $G$.

**Theorem 1.10.** Let $H$ be an invariant subgroup of a group $G$. The elements $Hs_1, Hs_2, Hs_3, \ldots, Hs_n; s_k \in G$; $k = 1, 2, \ldots, n$; $s_1 = 1$, form a group.

**Definition 1.10.** The group defined in Theorem 1.10 shall be called the quotient group of $G$, relative to $H$, and shall be denoted by $G/H$. The identity element of $G/H$ is found to be $H$ since

$$H(Hs_1) = HHs_1 = Hs_1,$$

and

$$Hs_1(H) = HHs_1 = Hs_1.$$

**Theorem 1.11.** The same quotient group is obtained from right cosets as from left cosets.

---

CHAPTER II

FUNDAMENTAL LEMMAS

Lemma 2.1. \([a,b][b,a] = 1\) or \([b,a] = [a,b]'\).
Proof: \([a,b][b,a] = aba'b'bab'a'\)
        \[= aba'ab'a'\]
        \[= abb'a'\]
        \[= aa'\]
        \[= 1.\]

Lemma 2.2. \([l,a] = [a,l] = 1\).
Proof: \([l,a] = 1al'a'\)
          \[= aa'\]
          \[= 1;\]
          \([a,l] = ala'l'\)
          \[= aa'\]
          \[= 1.\]

Lemma 2.3. \([a,a] = 1\)
Proof: \([a,a] = aa'\bar{a}'\)
          \[= aa'\]
          \[= 1.\]
Lemma 2.4. \[ bab' = [b,a]a. \]
Proof: \[
bab' = bab'(a'a) \\
= (bab'a')a \\
= [b,a]a.
\]

Lemma 2.5. \[ [a',b] = a'[b,a]a. \]
Proof: \[
[a',b] = a'bab' \\
= a'bab'(a'a) \\
= a'(bab'a')a \\
= a'[b,a]a.
\]

Lemma 2.6. \[ [a,b'] = b'[b,a]b. \]
Proof: \[
[a,b'] = ab'a'b \\
= (b'b)ab'a'b \\
= b'(bab'a')b \\
= b'[b,a]b.
\]

Lemma 2.7. \[ c[a,b]c' = [cac',cbc']. \]
Proof: \[
c[a,b]c' = c(aba'b')c' \\
= ca(c'c)b(c'c)a'(c'c)b'c' \\
= (cac')(cbc')(ca'c')(cb'c') \\
= (cac')(cbc')(cac')(cbc')' \\
= [cac',cbc'].
\]

Lemma 2.8. \[ [a,b]ba = ab. \]
Proof: \[
[a,b]ba = aba'b'ba \\
= aba'a \\
= ab.
\]
**Definition 2.1.** \([a, b, c] = a, [b, c]].\)

**Lemma 2.9.** \([a, bc] = [a, b]b[a, c]b'.\)

**Proof:**
\[a, bc] = a(bc)a'(bc)'
\[= abca'c'b'
\[= ab(a'a)ca'c'b'
\[= aba'(b'b)aca'c'b'
\[= (aba'b')b(aca'c')b'
\[= [a, b]b[a, c]b'.\]

**Lemma 2.10.** \([ab, c] = a[b, c]a'[a, c].\)

**Proof:**
\[ab, c] = (ab)c(ab)'c'
\[= abcb'a'c'
\[= abcb'(c'c)a'c'
\[= abcb'c'(a'a)ca'c'
\[= a(bcb'c')a'(aca'c')
\[= a[b, c]a'[a, c].\]

**Lemma 2.11.** \([a, b, c][b, c][a, c] = [ab, c].\)

**Proof:**
\[a, b, c][b, c][a, c] = [a, [b, c]][b, c][a, c]
\[= a[b, c]a'[b, c]'[b, c][a, c]
\[= a[b, c]a'[a, c]
\[= a(bcb'c')a'(aca'c')
\[= abcb'c'ca'c'
\[= abc'a'c'
\[= (ab)c(ab)'c'
\[= [ab, c].\]
Lemma 2.12. \([a,b][b,a,c][a,c] = [a,bc]\).

Proof: \([a,b][b,a,c][a,c] = [a,b][b,[a,c]][a,c]\)

\[= [a,b][b,a,c][a,b][a,c]\]

\[= [a,b][a,c][a,b][a,c]\]

\[= [a,b][a,c][a,b'][c][a,c]\]

\[= [a,b][a,c][a,b'][c][c][a,c]\]

\[= aba'b'baca'c'b'\]

\[= aba'aca'c'b'\]

\[= abca'c'b'\]

\[= a(bc)a'(bc)'\]

\[= [a,bc].\]
CHAPTER III

BASIC THEOREMS ON COMMUTATORS

**Theorem 3.1.** For elements $a, b \in G$, $[a, b] = 1$ if and only if $ab = ba$.

Proof: If $[a, b] = 1$, then

$$aba'b' = 1,$$

$$aba' = b,$$ and

$$ab = ba.$$  

Conversely, if $ab = ba$, then

$$aba' = b,$$ and

$$aba'b' = 1,$$ or

$$[a, b] = 1.$$  

Theorem 3.1 asserts that if $[a, b] = 1$ for arbitrary elements $a, b \in G$, $G$ is abelian.

**Theorem 3.2.** Let $U$ denote the subset of a group $G$ generated by the set of commutators of $G$, i.e., let $U$ denote the set of elements which may be obtained by forming products in such a manner that every factor of each product is a commutator of $G$. The set $U$ is a group.

Proof: If $a, b \in U$, then $ab \in U$. By definition of $U$, $a$ and $b$ are each a product of commutators; hence $ab$ is a product of commutators.
If \( a, b, c \in U \), then \( a(bc) = (ab)c \). Since \( a, b, c \) are each elements of the group \( G \), the associative law holds.

\( U \) contains the identity element \( 1 \). Consider commutator \([a,1]\), where \( a \in U \). By Lemma 2.2, \([a,1][a,1] = 1\); hence \( 1 \) is a product of commutators and contained in \( U \).

If \( g \in U, g' \in U \). Elements of \( U \) are products of commutators; therefore \( g \) can be written

\[
g = [a_1, b_1][a_2, b_2] \cdots [a_n, b_n],
\]

where \( a_i, b_i \in G, i = 1, 2, \cdots n \).

By Theorem 1.5, \( g' \) is found to be

\[
[a_n, b_n]' \cdots [a_2, b_2]'[a_1, b_1]',
\]

which finally, by Lemma 2.1, can be written

\[
[b_n', a_n] \cdots [b_2', a_2][b_1', a_1].
\]

The element \( g' \) is thus seen to be a product of commutators and therefore is contained in \( U \).

**Theorem 3.2.** The commutator operation is linked with multiplication by distributive laws if and only if the commutator of any pair of elements lies in the center. That is, for elements \( a, b, c \) of a group \( G \),

\[
[ab, c] = [b, c][a, c],
\]

and

\[
[a, bc] = [a, b][a, c]
\]

if and only if commutators commute.

**Proof:** I. From Lemma 2.10, the commutator

\[
[ab, c] = a[b, c]a'[a, c]
\]

for elements \( a, b, c \in G \).
If commutators commute, then
\[ [ab,c] = [b,c]aa'[a,c] = [b,c][a,c]. \]

Conversely, if
\[ [ab,c] = [b,c][a,c], \]
that is, if
\[ a[b,c]a'[a,c] = [b,c][a,c], \]
then
\[ a[b,c]a' = [b,c][a,c][a,c]; \]
and
\[ a[b,c]a' = [b,c]. \]

Thus
\[ a[b,c] = [b,c]a, \]
and \([b,c]\) lies in the center.

II. From Lemma 2.9, the commutator
\[ [a, bc] = [a, b]b[a, c]b' \]
for elements \(a, b, c \in G.\)

If commutators commute, then
\[ [a, bc] = [a, b][a, c]bb' = [a, b][a, c]. \]

Conversely, if
\[ [a, bc] = [a, b][a, c], \]
that is, if
\[ [a, b]b[a, c]b' = [a, b][a, c], \]
then
\[ b[a, c]b' = [a, b]'[a, b][a, c], \]
and

\[ b[a,c]b' = [a,c]. \]

Thus

\[ b[a,c] = [a,c]b \]

and \([a,c]\) lies in the center.

**Theorem 3.** If commutators commute, then

\[ [a,b,c][b,c,a][c,a,b] = 1 \]

for elements \(a,b,c\) of a group \(G\).

**Proof:**

\[ c[a,b]c' = caba'b'c' \]

\[ = caba'b'c'(bab'a'aba'b') \]

\[ = c(aba'b')c'(aba'b')(aba'b') \]

\[ = c[a,b]c'[a,b][a,b] \]

\[ = [c,[a,b]][a,b] \]

\[ = [c,a,b][a,b]. \quad (1) \]

Also,

\[ c[a,b]c' = caba'b'c' \]

\[ = ca(c'c)b(c'c)a'(c'c)b'c' \]

\[ = cac'cbc'ca'c'cb'c' \]

\[ = cac'cbc'(cbc'cac')' \]

\[ = cac'(a'a)cac'(b'b) \{ cac'(b' \]

\[ \quad b)cac'(a'a) \} ' \]

\[ = cac'a'acbc'b'(a'bcb'c'cbc' \\
\quad b'a)b \{ cbc'b'bcac'a'(b'aca'c' \\
\quad cac'a'b)a \} ' \]

\[ = cac'a'acbc'b'a'bcb'c'cbc'b'ab \]

\[ a'b'aca'c'cac'a'baca'c'b'bcb'c' \]
= (cac'a')a(cbc'b')(cbbc'b')'(cbc'b')ab(ba')'(aca'c')(cac'a')b(cac'
a')'b'(bcb'c')
= [c,a][a,c,b][c,b](aba'b')[c,a]'
=[[c,a],b][b,c]
= [c,a][a,c,b][c,b][a,b][c,a]'[b,c,a]'[c,b]'[c,b].

Since commutators commute by hypothesis, the product

\[ c[a,b]c' = [a,c,b][a,b][c,a][c,a]'[c,b]'[b,c,a]' = [a,c,b][a,b][b,c,a] \]  \hspace{1cm} (2)

and by equating (1) and (2), it is found that

\[ [c,a,b][a,b] = [a,c,b][a,b][b,c,a]' = [a,c,b][b,c,a]'[a,b]. \]

Thus

\[ [c,a,b] = [a,c,b][b,c,a]' \]  \hspace{1cm} (3)

Making use of equation (3), the expression

\[ [a,b,c][b,c,a][c,a,b] = [a,b,c][b,c,a][a,c,b][b,c,a]' = [a,b,c][a,c,b][b,c,a]' = [a,b,c][a,c,b] = [a,[b,c]][a,[c,b]]. \]

By Theorem 3.3,

\[ [a,[b,c]][a,[c,b]] = [a,[b,c][c,b]] = [a,1] = 1. \]

Therefore

\[ [a,b,c][b,c,a][c,a,b] = 1. \]
Theorem 3.5. The operation of forming commutators is associative in a group $G$, i.e.,

$$[[a,b],c] = [a,[b,c]]$$

if and only if the commutator subgroup $U$ of $G$ lies in the center of $G$.

Proof: If $U$ lies in the center of $G$, then

$$[[a,b],c] = [a,b][a,b]'c'$$
$$= [a,b][a,b]'cc'$$
$$= 1,$$

and

$$[a,[b,c]] = a[b,c]a'[b,c]'$$
$$= aa'[b,c][b,c]'$$
$$= 1.$$

Therefore,

$$[[a,b],c] = [a,[b,c]].$$

Conversely, suppose

$$[[a,b],c] = [a,[b,c]],$$

where elements $a,b,c$ are arbitrary. Let $c = b$. Then

$$[[a,b],b] = [a,[b,b]]$$
$$= [a,1]$$
$$= 1.$$

Since

$$[[a,b],b] = [a,b]b[a,b]'b',$$

$$[a,b]b[a,b]'b' = 1,$$ and

$$[a,b]' = b'[a,b]'b',$$ or
\[ [a,b]' = b'[b,a]b. \]

Furthermore, by Lemma 2.6,
\[ b'[b,a]b = [a,b'], \]

hence
\[ [a,b]' = [a,b']. \] \hspace{1cm} (1)

Now suppose \( a = b, b = a' \) in (1). Then
\[ [b,a']' = [b,a], \] or
\[ [b,a] = [b,a']', \] and
\[ [a,b]' = [a',b]. \] \hspace{1cm} (2)

Equating equations (1) and (2) results in
\[ [a',b] = [a,b'] \]

for arbitrary elements \( a',b \).

Now, by letting \( a = a' \),
\[ [a,b] = [a',b']. \] \hspace{1cm} (3)

Let us consider arbitrary elements \( a,b,c \) and equation (3). The relation
\[ [[[a,b],c] = [[[a,b]',c'] \]
\[ = [a,b]'c'[a,b]c, \]

which, by equations (2) and (1) becomes
\[ [[[a,b],c] = [a',b]c'[b,a'][c]. \] \hspace{1cm} (4)

Also, from equation (3),
\[ [a,[b,c]] = [a',[b,c]'] \]
\[ = a'[b,c]'a[b,c], \]

which, by equations (1) and (3) becomes
\[ [a,[b,c]] = a'[b,c']a[b',c']. \] \hspace{1cm} (5)

Now, by equating equations (4) and (5),
\[ [a', b']c'[b, a']c = a'[b, c']a[b', c'], \]

that is,
\[ a'bab'c'ba'b'ac = a'bc'b'cab'c'bc, \]

and thus
\[ ab'c'ba'b'a = c'b'cab'c'b. \]  \hspace{1cm} (6)

Multiplying equation (6) on the left by c, yields
\[ cab'c'ba'b'a = b'cab'c'b, \]

and successive right multiplication results in
\[ cab'c'ba'b'ab'cba'c'b = 1, \]

which may be written in the form
\[ c(ab')c'(ab')(ab')(ab')(ab')c'c'b = 1. \]

Thus
\[ [c, ab']b'[ab', c]b = 1, \text{ or} \]
\[ [[c, ab'], b'] = 1. \]

However, the elements \( a, b', c, \) and \( b \) are arbitrary since \( a, b, \) and \( c \) are arbitrary. Thus it is shown that the commutator of any pair of elements of \( G \) commutes with all of the elements of \( G \), i.e.,
\[ [c, ab']b' = b'[c, ab'] \]

and therefore the commutator subgroup \( U \) lies in the center.

**Theorem 2.6.** The commutator subgroup \( U \), of a group \( G \), is an invariant subgroup.

**Proof:** Let \( x \) be an element of \( G \), and suppose \([a, b]\) is a commutator of \( G \). Then
\[ x[a, b]x' = xaba'b'x' \]
\[ = xa(x'x)b(x'x)a'(x'x)b'x' \]
\[ = (xax')(xbx')(xa'x')(xb'x') \]
\[ = (xax')(xbx')(xax')(xbx')' \]
\[ = [xax', xbx']. \]

Now let \( u \) be any element from \( U \). Then
\[ u = [a_1, b_1][a_2, b_2] \cdots [a_n, b_n], \quad \text{and} \]
\[ xux' = x[a_1, b_1]x'x[a_2, b_2] \cdots x'x[a_n, b_n]x' \]
\[ = [xa_1x', xb_1x'][xa_2x', xb_2x'] \cdots [xa_nx', xb_nx']. \]

The transform of an element of \( U \) by an arbitrary element of \( G \) is a product of commutators and hence is in \( U \). \( U \) is therefore an invariant subgroup of \( G \).

**Theorem 3.7.** The quotient group \( G/H \) of the commutator group \( U \) is abelian.

**Proof:** The elements of \( G/H \) are the operations \( Ua \), where \( a \in G \). The commutator of two such operations may be written
\[ (Ua)(Ub)(Ua')(Ub') = UUabUUa'b' \]
\[ = UabUa'b' \]
\[ = UUaba'b' \]
\[ = Uaba'b'. \]

However,
\[ Uaba'b' = U, \]

since \( aba'b' \) is itself an element of \( U \). Hence in \( G/H \), every commutator is equal to \( U \) which is the unit element of that group, i.e., \( G/H \) is abelian. (Theorem 3.1)
Corollary 3.7. The commutator group $U$ is contained in every invariant subgroup which has an abelian quotient group.

Proof: Let $H$ be an invariant subgroup of $G$ whose quotient group is abelian. By Theorem 3.7, if 
\[[a,b] \in U,\]
then 
\[H[a,b] = H.\]
That is, $H$ contains the arbitrary element, $[a,b]$, and thus, $U$ is contained in $H$. 
BIBLIOGRAPHY

Books


Articles
