ORDERS OF CONJUGACY

IN GROUPS

By

Turki Mahmoud Said

Submitted in Partial fulfillment for the

Requirements of the Degree Master of Science

in the Mathematics Department of the

American University of Beirut

Beirut, Lebanon.

February, 1967

ORDERS OF CONJUGACY

IN GROUPS

Turki Mahmoud Said

ACKNOWLEDGMENT

To my Professor Peter Yff, I pay my deepest thanks for his valuable help and continuous encouragement in preparing this paper which, without his guidance, could not have come into being.

I am also indebted to Miss Mona Jabbour who typed this paper.

To Miss Hana', my fiancee, I present this paper.

ABSTRACT

In group theory, we have a definition for conjugate elements; namely, two elements x and y in a group G are conjugate if there exists an element a in G such that $y = a^{-1} x a$. In the present paper this will be called 1-conjugacy, as introduced in [1]. In [1] also, an extension of this definition is introduced; namely k-conjugacy (this will appear on p.8 in this paper) and how this concept is related to that of the number of commutators required to express an element in the commutator subgroup of G. A further study of the definition will give some results that will appear in this paper, some solutions will be mentioned for one of the basic theorems in [1], namely theorem 8 in this paper.

TABLE OF CONTENTS

CHAPTER I

SOME BASIC PROPERTIES OF GROUPS

Introduction:

As mentioned in the abstract, the purpose of this paper is to study an extension of the concept of conjugacy in a group called k-conjugacy[1;p.1]. Ideas introduced in [1] are employed to yield further results: of some examples, particularly permutation groups, are provided to illustrate the theory. We shall begin with a definition of a group and some immediate consequences. Known theorems will be ordinarily stated without proof.

Definition 1: A set G of elements (finite or infinite) with a single-valued binary operation between its elements is said to form a group G if the following conditions are satisfied:

C1: Closure of G under the binary operation;

To any ordered pair of elements a,b in G, there corresponds a unique element c in G, determined by the group operation. This correspondence will be denoted by multiplication: ab = c.

C2: Associativity of the operation;

For any three elements a,b,c in G; (ab)c = a(bc), which allows us to indicate the product without ambiguity as abc.

C3: Existence of an identity;

There exists an element e in G such that ea = ae = a for every a in G. e is called the identity element of G.

C4: Existence of inverses;

For any a in G, there exists a^{-1} in G such that $aa^{-1} = a^{-1}a = e$. a^{-1} is called the inverse of a.

Notice that in G1 and G2 the elements need not all be distinct. We list now some of the properties that are easily proved:

a) The associativity in G is true for any number of elements in a product. [2, p.4].

b) The identity element e, (e in G) is unique [2, p.5].

c) The inverse element a^{-1} of a is unique. [2, p.6].

d) The inverse of $a_1a_2 \cdots a_n$ is $a_n^{-1} a_{n-1}^{-1} \cdots a_2^{-1}a_1^{-1}$ [2, p.6].

Definition 2: The group G is said to be abelian (commutative) if for any two elements a,b in G. we have ab = ba.

Definition 3: The order of a finite group is the number of elements in the group.

Definition 4: A subset $H \subseteq G$ is said to be a subgroup of G if it forms a group under the operation of G.

We notice that every group has two trivial subgroups, namely, the subgroup consisting of the identity only and the whole group itself.

Definition 5: If H is any subgroup of G, and a is any fixed element in G, then the set aH consisting of all products ah(h in H) is called a left coset of H.

Right cosets are analogously defined.

Theorem 1: If H is a subgroup and if r and s are any two elements of G, then the cosets Hr and Hs are identical if and only if rs^{-1} is in H; otherwise they have no element in common.

Similarly the cosets rH and sH are identical if and only if $s^{-1}r$ is in H; otherwise they have no element in common.

Proof: See [2, P. 34].

Definition 6: A subgroup N of G is said to be normal in G if $a^{-1}Na = N$ for every a in G, or Na = aN, so that every left coset of N is also a right coset, and vice-versa.

Definition 7: If N is normal in G, then we define the factor group G/N as the set of all disjoint cosets of N in G, under the operation NaNb = Nab for every a,b in G.

For a discussion of the factor group see [2, p.102].

Definition 8: Two elements x,y in G are said to be conjugate if there exists an element a in G such that $y = a^{-1}xa$.

The element a is called the transforming element; i.e., it transforms x to $a^{-1}x\,a$.

Theorem 3: Conjugacy is an equivalence relation.

Proof: [see 2, p.96].

Definition 9: For any two elements a,b in G, the element $a^{-1}b^{-1}ab$ is called the commutator of a and b; we denote it by the letter c.

It is obvious from the definition that c = e if and only if ab = ba, which is the case in abelian groups; therefore in

any abelian group the only commutator is the identity element. But in general if a,b run through all possible values in G (independently), then we will have g^2 commutators (where g is the order of G), and these g^2 commutators can't be all distinct, (since $g^2 > g$ and G is closed). But e is always one of them (i.e. e is e commutator since $e = a^{-1}e^{-1}ae$, a in G), and also the inverse of every commutator is one of them, since if $a^{-1}b^{-1}ab$ is there, then $b^{-1}a^{-1}ba$ is also there. This set of commutators is not necessarily subgroup, since it is possible that the product of two commutators is not a commutator [3, p.39], i.e. the set is not necessarily closed under multiplication. However, since any set of elements in G generates a subgroup of G, the following definition is valid.

Definition 10: The set of all commutators in a group generates a subgroup, which is called the commutator subgroup.

This subgroup is denoted by C and it has the following properties:

C is normal in G, G/C is abelian and if H is normal in G, then G/H is abelian if and only if H contains C.

For a proof of these, see [2, p.105].

We note also that triple commutators $a^{-1}b^{-1}c^{-1}abc$ and n-fold commutators may be defined. In fact $a^{-1}b^{-1}c^{-1}abc$ is an ordinary commutator since

$$a^{-1}b^{-1}c^{-1}abc = (ba)^{-1}(bc)^{-1}(ba)(bc).$$

However, $a^{-1}b^{-1}c^{-1}d^{-1}abcd$ is not an ordinary commutator, since there exist groups in which the product of two commutators is not always a commutator and if we let $a^{-1}b^{-1}ab$ and $c^{-1}d^{-1}cd$ be two such commutators, then

$$a^{-1}b^{-1}ab\ c^{-1}d^{-1}cd = (cb^{-1})^{-1}(abc^{-1})^{-1}(cb^{-1}a^{-1})^{-1}d^{-1}(cb^{-1})(abc^{-1})(cb^{-1}a^{-1}b)d$$

$$= a_1^{-1}\ a_2^{-1}\ a_3^{-1}\ a_4^{-1}\ a_1\ a_2\ a_3\ a_4$$

which is not a commutator.

Therefore a product $a_1^{-1}\ldots\ldots a_k^{-1}\ a_1\ldots a_k$ can't always be reduced to a commutator if $k > 3$.

It may be shown that C is the set of elements that can be written in the form $a_1^{-1}a_2^{-1}\ldots\ldots\ldots a_k^{-1}\ a_1a_2\ \ldots\ a_k$. In fact the next theorem from [1] proves even more.

Theorem 4: a) Any product of k commutators in a group G is expressible in the form

$$a_1^{-1}a_2^{-1}\ \ldots\ a_{2k}^{-1}\ a_1a_2\ \ldots\ldots\ a_{2k}\ \text{(every } a_i \in G\text{)}.$$

b) Conversely, the element $a_1^{-1}\ldots\ldots a_m^{-1}\ a_1\ \ldots\ a_m$, in which $m = 2k$ or $2k + 1$, may be written as a product of k commutators.

Proof:

a) when $k = 1$, then $a_1^{-1}a_2^{-1}\ a_1a_2$ is a commutator [Def. 9]; i.e., the statement is true for $k = 1$. Now, apply induction; i.e., assume it true for $k = n$ and prove it for $k = n + 1$.

Let $c_1, c_2, \ldots c_n$, and $u^{-1}v^{-1}\ uv$ be $n + 1$ commutators. Then

$$u^{-1}v^{-1}\,uv(c_1c_2\cdots c_n) = u^{-1}v^{-1}\,uv(a_1^{-1}\,a_2^{-1}\,\cdots\,a_{2n}^{-1}\,a_1a_2\cdots a_{2n}),$$

(by assumption for k = n)

$$= (a_1v^{-1})^{-1}(uva_1^{-1})^{-1}(a_1v^{-1}u^{-1}v)^{-1}a_2^{-1}a_3^{-1}\cdots a_{2n}^{-1}(a_1v^{-1})(uva_1^{-1})$$

$$(a_1v^{-1}u^{-1}v)a_2a_3\cdots a_{2n}$$

$$= b_1^{-1}\cdots b_{2n+2}^{-1}\,b_1\cdots b_{2n+2},$$

where

$$b_1 = a_1v^{-1},$$

$$b_2 = u\,v\,a_1^{-1},$$

$$b_3 = a_1\,v^{-1}\,u^{-1}\,v,$$

$$b_i = a_{i-2} \quad \text{for} \quad i = 4,5,\ldots,2n+2.$$

So the statement is true for $k = n+1$ and thus for all k.

b) Since $a_1^{-1}\,a_2^{-1}\,a_1a_2$ and $a_1^{-1}\,a_2^{-1}\,a_3^{-1}\,a_1a_2a_3 =$

$$= (a_2a_1)^{-1}(a_2a_3)^{-1}(a_2a_1)(a_2a_3)$$

are both commutators; the statement is true when $m = 2$ or 3. We use induction on m. Suppose that the statement is true for $m = r$; then

$$a_1^{-1}\,a_2^{-1}\cdots\cdots\,a_r^{-1}\,a_{r+1}^{-1}\,a_{r+2}^{-1}\,a_1a_2\cdots\cdots\,a_ra_{r+1}a_{r+2}$$

$$= a_1^{-1}\cdots\,a_r^{-1}\,a_1\cdots a_r(a_{r+1}a_1\cdots a_r)^{-1}(a_{r+1}a_{r+2})^{-1}(a_{r+1}a_1\cdots a_r)$$

$$(a_{r+1}a_{r+2}).$$

But by assumption $a_1^{-1} \ldots\ a_r^{-1}\, a_1 \ldots\ a_r$ may be written as $\frac{1}{2}r$ or $\frac{1}{2}(r-1)$ commutators, according as r is even or odd; and the remaining part is one single commutator. Therefore the statement is true for $m = r+2$, and thence true for all m.

CHAPTER II

k-CONJUGACY

The results of this chapter are taken from [1]. Looking back on Definition 8, the ordinary conjugacy introduced there will be called, from hereon, 1-conjugacy. For $k > 1$, k-conjugacy is defined as follows.

Definition 11: For two elements x,y in G, we say that y is k-conjugate to x (written $y \underset{k}{\sim} x$) if there exist two elements r,s in G such that $y = r^{-1}xs$ and $s \underbrace{\sim \cdots \sim}_{k-1} r$.

It is consistent with this definition to regard 0-conjugacy as equality.

We mention now some of the theorems that are in [1] with their proofs.

Theorem 5: k-conjugacy has the following properties:

a) If $y \underset{k}{\sim} x$, then $y \underset{n}{\sim} x$ for every $n > k$.

b) k-conjugacy is reflexive.

c) k-conjugacy is symmetric.

d) If $y \underset{k}{\sim} x$, then $y^{-1} \underset{k}{\sim} x^{-1}$.

Proof:

a) Let $y \underset{k}{\sim} x$, but $y = x^{-1} x y$, then $y \underbrace{\sim \cdots \sim}_{k+1} x$ and the proof is complete using induction.

b) $x \underset{1}{\sim} x$ (Theorem 3). Therefore $x \underset{k}{\sim} x$ for every $k > 1$, as proved in a).

using property a) and the proof is complete by induction.

c,d) Let us use induction.

If $y \underset{1}{\sim} x$, then $x \underset{1}{\sim} y$ (Theorem 3), and $y^{-1} \underset{1}{\sim} x^{-1}$; since $y = a^{-1} x a$, then $y^{-1} = a^{-1}x^{-1}a$; i.e., $y^{-1} \underset{1}{\sim} x^{-1}$.

Assume now the statement is true for $x = n$ and prove it for $k = n+1$.

Let $v \underset{n}{\sim} u$ and $y = u^{-1} x v$; i.e., $y \underbrace{\sim}_{n+1} x$, then $x = u y v^{-1}$, but $v^{-1} \underset{n}{\sim} u^{-1}$ (by assumption) and thence $x \underbrace{\sim}_{n+1} y$. Also $y^{-1} = v^{-1}x^{-1}u$, but $u \underset{n}{\sim} v$, and thence $y^{-1} \underbrace{\sim}_{n+1} x^{-1}$. Hence the statement is true for every k.

<u>Theorem 6:</u> $y \underset{k}{\sim} x$ if and only if there exist $a_1, a_2, \ldots, a_{k+1}$ such that $x = a_1 a_2 \cdots a_{k+1}$ and $y = a_{k+1} a_k \cdots a_2 a_1$

Proof:

a)

Let $x = a_1a_2\cdots a_{k+1}$ and $y = a_{k+1}a_k \cdots a_2a_1$.

Since $a_2a_1 = a_1^{-1} (a_1a_2)a_1$, then $a_2a_1 \underset{1}{\sim} a_1a_2$, hence $y \underset{1}{\sim} x$ when $k = 1$. Assume that $y \underset{m}{\sim} x$ when $k = m$ and prove $y \underbrace{\sim}_{m+1} x$ when $k = m + 1$; i.e., if $y = a_{m+2}a_{m+1}\cdots a_1$ and

$x = a_1a_2 \cdots a_{m+2}$, then $y \underbrace{\sim}_{m+1} x$.

Consider

$$a_{m+2}a_{m+1}\cdots a_1 = (a_1 \cdots a_{m+1})^{-1}(a_1 \cdots a_{m+2})(a_{m+1}\cdots a_1).$$

Therefore

$y \underbrace{\sim}_{m+1} x$ when $k = m$ (by assumption of induction and definition 7)

Therefore

$y \underset{k}{\sim} x$ for every k.

b)

Let $y \underset{k}{\sim} x$. When $k = 1$, then $y = a^{-1}(xa)$ and $x = (xa)a^{-1}$ therefore $y = a_2a_1$ and $x = a_1a_2$, therefore the statement is true for $k = 1$. Let us use induction. Assume the statement is true for $k = m$.

Let $y \overbrace{\underset{m+1}{\sim}} x$; i.e., $y = u^{-1} x v$ where $v \underset{m}{\sim} u$, then $v = a_{m+1} a_m \cdots a_2a_1$ and $u = a_1a_2 \cdots a_{m+1}$ by assumption of induction.

Now select a_{m+2} such that $x = u\, a_{m+2}$, which implies that $y = a_{m+2} v$; i.e., $x = a_1a_2 \cdots a_{m+1} a_{m+2}$ and $y = a_{m+2} a_{m+1} \cdots a_2a_1$.

Therefore the statement is true for $k = m+1$ and hence for all k.

<u>Theorem 7:</u> If $y \underset{k}{\sim} x$, then x equals y times $\frac{1}{2}k$ or $\frac{1}{2}(k+1)$ commutators according as k is even or odd. Conversely, if x equals y times n commutators, then $y \underset{2n}{\sim} x$.

Proof:

a) $x = y(y^{-1}x)$; let us find the value of $y^{-1}x$.

Since $y \underset{k}{\sim} x$, then $y = a_{k+1} \cdots a_1$ and $x = a_1 \cdots a_{k+1}$ (Theorem 2) therefore

$$y^{-1}x = a_1^{-1} \cdots a_{k+1}^{-1} a_1 \cdots a_{k+1} \text{ (property d, p.2)}$$

= The product of $\frac{1}{2}k$ or $\frac{1}{2}(k+1)$ commutators, depending upon k even or odd (Theorem 4).

Therefore x equals y times $\frac{1}{2}k$ or $\frac{1}{2}(k+1)$ commutators according as k is even or odd.

b) Let $x = yc_1 \cdots c_n$, where each c_i is a commutator.

If $n = 1$, then $x = y\,c_1 = y\,a^{-1}b^{-1}\,ab =$

$$= (yay^{-1})^{-1}y(yb)^{-1}(yay^{-1})(yb)$$

Therefore

$$x \underset{2}{\sim} y \qquad \text{(Definition 11)}$$

Now we use induction.

Assume that $y \underset{2r}{\sim} x$, when $n = r$, and prove it for $n = r+1$.

If

$$n = r + 1,$$

then

$$x = y(c_1c_2 \cdots c_{r+1}) = (yc_1)(c_2 \cdots c_{r+1}),$$

so

$$x \underset{2r}{\sim} yc_1 \cdots \text{(by induction assumption)},$$

and

$$x = u^{-1}(yc_1)v \quad \text{where } v \underset{2r-1}{\sim} u.$$

But since $yc_1 \underset{2}{\sim} y$, $yc_1 = s^{-1}\,y\,t^{-1}\,st$,

therefore

$$x = u^{-1}(s^{-1}\,y\,t^{-1}\,st)v = u^{-1}s^{-1}\,y\,t^{-1}\,su\,u^{-1}\,t\,v$$

$$= (su)^{-1}\,y\,\{t^{-1}(su)(u^{-1}t\,v)\}\,.$$

Notice that $u^{-1}\,t\,v \underset{2r}{\sim} t$ since $v \underset{2r-1}{\sim} u$. Therefore $t^{-1}(su)(u^{-1}\,t\,v) \underset{2r+1}{\sim} (su)$ and therefore $x \underset{2r+2}{\sim} y$, hence $y \underset{2r+2}{\sim} x$.

Therefore the statement is true for $n = r+1$ and hence for all n.

Corollary 1: If $y \underset{k}{\sim} x$, then $y^{-1}\,x$ is in C.

Proof: Obvious.

Theorem 8: Let there be a fixed k such that $t \in C$ implies $t = a_1^{-1} \cdots\cdots a_k^{-1}a_1 \cdots a_k$ (we may assume k even), then k-conjugacy

is an equivalence relation separating G into the cosets of C. Furthermore, each element of C is expressible as a product of $\frac{1}{2}k$ commutators.

Proof:

We prove first that k could be assumed even. If k is even, then we are finished. But if k is odd, then using theorem 4, part b), we can write $t = a_1^{-1} \cdots a_k^{-1} a_1 \cdots a_k$ as a product of $\frac{1}{2}(k-1)$ commutators, and then using part a) of the same theorem then, we can write the product of $\frac{1}{2}(k-1)$ commutators as $b_1^{-1} \cdots b_{k-1}^{-1} b_1 \cdots b_{k-1} = t$ and k-1 is even.

Now, for any k, if $y \underset{k}{\sim} x$, then $y^{-1} x$ is in C (corollary to Theorem 7), so x and y are in the same coset of C (Theorem 1).

Conversely, assume $y^{-1} x$ is in C; then by hypothesis $y^{-1} x = a_1^{-1} a_2^{-1} \cdots a_k^{-1} a_1 a_2 \cdots a_k$ and therefore, a product of $\frac{1}{2}k$ commutators (Theorem 4). Therefore $y \underset{k}{\sim} x$, and it follows that k-conjugacy is an equivalence relation.

CHAPTER III

FURTHER THEOREMS ON k-CONJUGACY

Again all elements in this chapter are assumed to be in a group G.

Theorem 9a: If $y \underset{k}{\sim} x$, then $cy \underset{k}{\sim} cx$ or $cy \underset{k+1}{\sim} cx$ according as k is even or odd.

Proof:

if $y \underset{1}{\sim} x$, then $y = a^{-1} x a$.

$$cy = ca^{-1} x a$$

$$= ca^{-1} c^{-1} cx a$$

$$= (c a c^{-1})^{-1} (cx) a$$

Therefore

$$cy \underset{2}{\sim} cx \text{ , since } a \underset{1}{\sim} c a c^{-1}$$

if $y \underset{2}{\sim} x$, then $y = (aba^{-1})^{-1} x b$

$$= ab^{-1} a^{-1} x b$$

$$cy = cab^{-1} a^{-1} x b$$

$$= cab^{-1} a^{-1} c^{-1} c x b$$

$$= \left(caba^{-1} c^{-1}\right)^{-1} (cx) b$$

$$= \left\{(ca) b(ca)^{-1}\right\}^{-1} (cx) b$$

therefore

$$cy \underset{2}{\sim} cx \ ; \text{ since } b \underset{1}{\sim} (ca)b(ca)^{-1}.$$

Therefore the statement is true for $k = 1,2$.

Let us use induction and assume that the theorem is true for all $k < n$. Now let $y \underset{n}{\sim} x$; i.e.,

$$y = r^{-1} x s, (s \underset{n-1}{\sim} r)$$

therefore

$$cy = cr^{-1} c^{-1} cx s$$

$$= (crc^{-1})^{-1} (cx) s$$

But since

$$s = t^{-1} ru, (u \underset{n-2}{\sim} t,)$$

$$r = tsu^{-1}, \text{ and } crc^{-1} = (ct) s(cu)^{-1}$$

By the induction hypothesis, $cu \underset{n-2}{\sim} ct$ if n is even, and $cu \underset{n-1}{\sim} ct$ if n is odd. Hence

$$crc^{-1} \underset{n-1}{\sim} s \text{ if n is even, and}$$

$$crc^{-1} \underset{n}{\sim} s \text{ if n is odd.}$$

Finally,

$$cy \underset{n}{\sim} cx \text{ if n is even,}$$

and

$$cy \underset{n+1}{\sim} cx \text{ if n is odd.}$$

An alternative proof is provided by the use of theorem 6 and it is as follows:

Since $y \underset{k}{\sim} x$, there exist $a_1, \ldots, a_{k+1}$ such that

$$x = a_1 \ldots a_{k+1} \text{ and } y = a_{k+1} \ldots a_1.$$

If k is even, then

$$cx = (ca_1)(a_2c^{-1})(ca_3)(a_4c^{-1})\ldots.(a_kc^{-1})(ca_{k+1})$$

and

$$cy = (ca_{k+1})(a_kc^{-1})(ca_{k-1})\ldots.(a_2c^{-1})(ca_1).$$

Therefore

$$cy \underset{k}{\sim} cx \text{ , (Theorem 6).}$$

If k is odd, then

$$cx = (ca_1)(a_2c^{-1})(ca_3)\ldots.(a_{k-1}c^{-1})(ca_k)(a_{k+1}c^{-1})(c);$$

$$cy = (c)(a_{k+1}c^{-1})(ca_k)\ldots.(ca_3)(a_2c^{-1})(ca_1).$$

Therefore

$$cy \overbrace{\quad}^{k+1} cx \text{ ,(Theorem 6).}$$

<u>Corollary 2:</u> If $y \underset{k}{\sim} x$, then $yc \underset{k}{\sim} xc$ or $yc \overbrace{\quad}^{k+1} xc$ according as k is even or odd.

Proof:

Since $y \underset{k}{\sim} x$, then $y^{-1} \underset{k}{\sim} x^{-1}$ ... (Property d, Theorem 5)

and hence

$$c^{-1}y^{-1} \underset{k}{\sim} c^{-1}x^{-1} \text{ , if k is even}$$

or

$$c^{-1}y^{-1} \overbrace{\quad}^{k+1} c^{-1}y \text{ , if k is odd.}$$

} (Theorem 9a).

Therefore

$$yc \underset{k}{\sim} xc$$

or

$$yc \overbrace{\quad}^{k+1} xc$$

} (Property d, Theorem 5).

<u>Theorem 9b</u>: If $y \underset{k}{\sim} x$, then $cy \overbrace{\quad}^{k+1} xc$.

Proof:

Since $y \underset{k}{\sim} x$, there exist $a_1, a_2, \ldots a_{k+1}$ such that

$$x = a_1 \cdots a_{k+1}$$

and

$$y = a_{k+1} \cdots a_1,$$

therefore

$$cy = c\, a_{k+1} \cdots a_1,$$

$$xc = a_1 \cdots a_{k+1}\, c.$$

Therefore

$$cy \underset{k+1}{\sim} xc \quad \text{(Theorem 6)}.$$

Theorem 10a: $(ab)^n \underset{n}{\sim} b^n a^n$

Proof:

The proof here depends upon theorem 6 and so let us write the first few cases which indicte a pattern in the factorization of $(ab)^n$ and $b^n a^n$.

$(ab)^1 = ab$ $\qquad$ $b^1a^1 = ba$

$(ab)^2 = a(ba)b$ $\qquad$ $b^2a^2 = b(ba)a$

$(ab)^3 = a(ba)(bab^{-1})b^2$ $\qquad$ $b^3a^3 = b^2(bab^{-1})(ba)a$

$(ab)^4 = a(ba)(bab^{-1})(b^2ab^{-1})b^2$ $\qquad$ $b^4a4 = b^2(b^2ab^{-1})(bab^{-1})(ba)a$

$(ab)^5 = a(ba)(bab^{-1})(b^2ab^{-1})(b^2ab^{-2})b^3$ $\qquad$ $b^5a^5 = b^3(b^2ab^{-2})(b^2ab^{-1})(bab^{-1})(ba)a$

In general assume $(ab)^k \underset{k}{\sim} b^k a^k$.

Now let $(ab)^k = c_1 \cdots c_{k+1}$ and $b^k a^k = c_{k+1} \cdots c_1$ where all c_i are in G. We may also assume that $c_{k+1} = b^r$, since

this is true when $k = 1,2,3,4,5$.

Then

$$c_k \cdots c_1 = b^{k-r} a^k.$$

Now

$$(ab)^{k+1} = c_1 \cdots c_k (b^r ab^{r-k}) b^{k+1-r}$$

and

$$b^{k+1} a^{k+1} = b^{k+1-r} (b^r ab^{r-k}) c_k \cdots c_1;$$

i.e.,

$$(ab)^{k+1} = d_1 \cdots d_{k+2}$$

and

$$b^{k+1} a^{k+1} = d_{k+2} \cdots d_1,$$

where

$$d_i = c_i \text{ for all } i = 1,2,\cdots k,$$

$$d_{k+1} = b^r ab^{r-k},$$

and

$$d_{k+2} = b^{k+1-r}.$$

Therefore

$$(ab)^{k+1} \underset{k+1}{\sim} b^{k+1} a^{k+1},$$

and hence

$$(ab)^n \underset{n}{\sim} b^n a^n \text{ is true for all } n.$$

<u>Corollary 3:</u> $b^n a^n (ab)^{-n}$ is the product of $\frac{1}{2}(n+1)$ or $\frac{1}{2}n$ commutators according as n is odd or even.

Proof:

Apply Corollary 1 to Theorem 7 and Theorem 6.

We introduce now two lemmas that will be used in proving the next theorem.

<u>Lemma 1:</u> The conjugate of a commutator is a commutator.

Proof:

$$x^{-1}(a^{-1}b^{-1}ab)x = x^{-1}a^{-1}b^{-1}ab\ x$$

$$= x^{-1}\ a^{-1}\ x\ x^{-1}b^{-1}x\ x^{-1}\ ax\ x^{-1}bx$$

$$= (x^{-1}ax)^{-1}(x^{-1}bx)^{-1}(x^{-1}ax)(x^{-1}bx),$$

which is a commutator (Definition 9).

Lemma 2: The conjugate of a product of a set of n commutators is a product of a set of n commutators.

Proof:

Obvious, using the method in Lemma 1.

Theorem 10b: $(ab)^n \underset{n}{\sim} a^n\ b^n$ or $(ab)^n \underset{n-1}{\sim} a^n\ b^n$ according as n is even or odd.

Proof:

We will depend upon the previous theorem and its corollary. Consider the product $a^n\ b^n\ (ab)^{-n}$:

$$a^n b^n (ab)^{-n} = a\left\{ a^{n-1}\ b^{n-1}(ba)^{-(n-1)}\right\} a^{-1}$$

but $a^{n-1}\ b^{n-1}(ba)^{-(n-1)}$ is the product of $\frac{1}{2}(n-1)$ or $\frac{1}{2}n$ commutators, according as n is odd or even (Corollary 3) therefore $a\left\{a^{n-1}\ b^{n-1}\ (ba)^{-(n-1)}\right\} a^{-1}$ is also the product of $\frac{1}{2}(n-1)$ or $\frac{1}{2}n$ commutators. (Lemma 2).

Therefore $(ab)^n \underset{n}{\sim} a^n\ b^n$ or $(ab)^n \underset{n-1}{\sim} a^n\ b^n$ according as n is even or odd (Theorem 7).

Theorem 11a: If $y \underset{k}{\sim} x$ and $s \underset{m}{\sim} r$, then $sy \underset{m+k}{\sim} rx$ if m and k

are both even, otherwise $sy \underbrace{\qquad}_{m+k+1} rx$.

Proof: Let

$$k = 1 : \quad y = a^{-1} xa,$$

$$sy = sa^{-1} x a = sa^{-1} r^{-1} (rx) a$$

$$= (ras^{-1})^{-1} (rx) r^{-1} (ras^{-1})s.$$

Now

$$r^{-1}(ras^{-1})s \underbrace{\qquad}_{m+1} ras^{-1}, \text{ because } s \underbrace{\sim}_{m} r.$$

Therefore

$$sy \underbrace{\qquad}_{m+2} rx.$$

Now assume $sy \underbrace{\qquad}_{m+k+1} rx$ for $k < n$, and let $k = n$;

then

$$y = u^{-1} x^{-1} t^{-1} uv \qquad (v \underbrace{\qquad}_{n-2} t)$$

$$sy = (rus^{-1})^{-1} (rx) (rt)^{-1} (rus^{-1})(sv)$$

now

$$(rt)^{-1}(rus^{-1})(sv) \underbrace{\qquad}_{n+m} rus^{-1}, \text{ since } sv \underbrace{\qquad}_{n+m-1} rt.$$

Therefore

$$sy \underbrace{\qquad}_{n+m+1} rx.$$

Thus $(k+m+1)$-conjugacy is verified for all cases. We show now that the reduction is possible when k,m are even; i.e., we prove $sy \underbrace{\qquad}_{m+k} rx$.

Let k and m be even. We could begin with the trivial case $k = m = 0$, but let us take $k = 2$ and any m :

$$y = (a^{-1}ba)^{-1}\, xb, \qquad (s \underset{m}{\sim} r)$$

$$sy = s(a^{-1}ba)^{-1}\, r^{-1}(rx)b$$

$$= (as^{-1})^{-1}\, b(ar^{-1})\, (rx)b.$$

Now $as^{-1} \underset{m}{\sim} ar^{-1}$ (Theorem 9a), so $b \underbrace{\sim}_{m+1} (as^{-1})^{-1}\, b(ar^{-1})$.

Therefore

$$sy \underbrace{\sim}_{m+2} rx.$$

Let the result be true for $k = 2n$, and we try $k = 2n + 2$:

$$y = u^{-1}\, x\, v, \qquad (v \underbrace{\sim}_{2n+1} u)$$
$$sy = su^{-1}\, r^{-1}\, (rx)\, v$$

$$= s(q^{-1}vt)^{-1}\, r^{-1}\, (rx)v \qquad (t \underset{2n}{\sim} q)$$

$$= (ts^{-1})^{-1}\, v^{-1}\, (qr^{-1})(rx)\, v$$

$$= \left\{(qr^{-1})^{-1}\, v\, (ts^{-1})\right\}^{-1}\, (rx)v.$$

Now $v \underbrace{\sim}_{m+2n+1} (qr^{-1})^{-1}\, v\, (ts^{-1})$, since $qr^{-1} \underbrace{\sim}_{m+2n} ts^{-1}$ (assumption of induction).

Therefore

$$sy \underbrace{\sim}_{m+2n+2} rx.$$

and the result follows.

Theorem 11b: If $y \underset{k}{\sim} x$ and $s \underset{m}{\sim} r$, then $ys \underbrace{\sim}_{m+k+1} rx$.

Proof:

$y \underset{k}{\sim} x$, then there exist $a_1, a_2, \ldots a_{k+1}$ such that

$$x = a_1 \ldots a_{k+1} \text{ and } y = a_{k+1} \ldots a_1 \text{ (Theorem 6)}.$$

$S \underset{m}{\sim} r$; then there exist $b_1, b_2, \ldots b_{m+1}$ such that

$$r = b_1 b_2 \ldots b_{m+1} \quad \text{and} \quad s = b_{m+1} \ldots b_1;$$

therefore

$$ys = a_{k+1} \ldots a_1 \, b_{m+1} \ldots b_1$$

and

$$rx = b_1 \ldots b_{m+1} \, a_1 \ldots a_{k+1} .$$

Therefore

$$ys \overbrace{\sim}^{k+m+1} rx \quad \text{(Theorem 6)} .$$

Theorem 11c: If $y \underset{k}{\sim} x$ and $s \underset{m}{\sim} r$, then $y \overbrace{\sim}^{m+k} r^{-1} xs$ if m is even and k odd, otherwise

$$y \overbrace{\sim}^{k+m+1} r^{-1} xs.$$

Proof:

If $y \underset{k}{\sim} x$, then $y = t^{-1} x u$, $(u \overbrace{\sim}^{k-1} t)$

$$= t^{-1} r r^{-1} xs \, s^{-1} u$$

$$= t^{-1}$$

$$= (r^{-1} t)^{-1} (r^{-1} xs)(s^{-1} u).$$

Let us consider two cases:

a) m is odd,

$u \overbrace{\sim}^{k-1} t$, then $s^{-1} u \overbrace{\sim}^{k+m} r^{-1} t$ (Theorem 11a).

Therefore

$$y \overbrace{\sim}^{k+m+1} r^{-1} x s.$$

b) m is even,

$u \overbrace{\sim}^{k-1} t$, then $s^{-1} u \overbrace{\sim}^{k+m-1} r^{-1} t$ or $s^{-1} u \overbrace{\sim}^{k+m} r^{-1} t$ according as k is odd or even.

Therefore $y \overbrace{\ }^{k+m} r^{-1}$ x s or $y \overbrace{\ }^{k+m+1} r^{-1}$ x s according as k is odd or even. Combining the two cases, we get the result.

Theorem 12: If $y \underset{k}{\sim} x$ and $Z \underset{m}{\sim} y$, then $Z \overbrace{\ }^{k+m-1} x$ if k and m are odd, otherwise $Z \overbrace{\ }^{k+m} x$.

Proof:

$y \underset{k}{\sim} x$; then $y = r^{-1}$ xs (where $s \overbrace{\ }^{k-1} r$);

$Z \underset{m}{\sim} y$; then $Z = t^{-1}$ yu (where $u \overbrace{\ }^{m-1} t$)

$= t^{-1} r^{-1}$ xsu

$= (rt)^{-1}$ (x) (su).

But

$su \overbrace{\ }^{k+m-2} rt$, if k, m are odd, otherwise $su \overbrace{\ }^{k+m-1} rt$ (Theorem 11a).

Therefore $Z \overbrace{\ }^{k+m-1} x$ if k, m are odd, otherwise $Z \overbrace{\ }^{k+m} x$.

Theorem 12 indicates that k-conjugacy is not necessarily transitive. Taking m = k, we see that $y \underset{k}{\sim} x$ and $z \underset{k}{\sim} y$ imply $Z \overbrace{\ }^{2k-1} x$ or $Z \underset{2k}{\sim} x$. While there exist cases in which (2k-1)-conjugacy or 2k-conjugacy may be reduced to k-conjugacy, the following theorem (from [1]) shows that the reduction is not possible in general.

Theorem 13: k-conjugacy, for $k > 1$, is not always transitive.

Proof:

Consider e, the identity element in G, and $x = a^{-1} b^{-1}$ ab, then $e = ax\ b^{-1} a^{-1}$ b and so $e \underset{2}{\sim} x$. Conversely, if $e = c^{-1}$ y d^{-1} cd, then $y = cd^{-1} c^{-1}$ d. Therefore e is 2-conjugate to an element if

and only if the element is a commutator.

There exist groups in which the product of two commutators is not a commutator [4,p.55]. Let $x = (a^{-1} b^{-1} ab)(c^{-1} d^{-1} cd)$ be such an element; then $dxd^{-1} = d(a^{-1} b^{-1} ab)c^{-1} d^{-1} c$, so $dxd^{-1} \underset{2}{\sim} a^{-1} b^{-1} ab$. Now $e \underset{2}{\sim} a^{-1} b^{-1} ab$, but **e** is not 2-conjugate to dxd^{-1} since the later, like x, is not a commutator.

Therefore 2-conjugacy is not always transitive. Since 2-conjugacy implies k-conjugacy for all $k > 2$, the result holds for all $k > 1$.

We will study now the product $a = a_1 \dots a_k$ (a_i in G) and how it is related in terms of conjugacy to a permuted product $a' = a'_1 \dots a'_k$ (the same a_i but in a different order), and as special cases we will study $a_1^k \dots a_n^k$ related with $(a_1 \dots a_n)^k$ or $(a_n \dots a_1)^k$. We introduce first a basic theorem which gives us the key for reaching our goal.

Theorem 14: If any two factors of the product $a = a_1 \dots a_n$ are interchanged, the resulting element is ordinarily 2-conjugate to a. An exceptional case occurs when $n = 2$; i.e., $a_1 a_2 \widetilde{1} a_2 a_1$.

Proof:

Let us interchange a_s and a_r, assuming $r < s$. Then

$a' = a_1 \dots a_{r-1} a_s a_{r+1} \dots a_{s-1} a_r a_{s+1} \dots a_n = a_1 \dots a_n x^{-1} y^{-1} xy$

where

$$\left.\begin{aligned} x &= (a_r \dots a_n)^{-1} (a_{r+1} \dots a_{s-1})^{-1} a_s^{-1} (a_r \dots a_n) \\ y &= (a_r \dots a_n)^{-1} (a_{r+1} \dots a_{s-1})^{-1} a_r^{-1} (a_r \dots a_n) \end{aligned}\right\} \text{ if } s > r+1$$

and

$$\left.\begin{aligned} x &= (a_r \dots a_n)^{-1} a_s^{-1} (a_r \dots a_n) \\ y &= (a_r \dots a_n)^{-1} a_r^{-1} (a_r \dots a_n) \end{aligned}\right\} \text{ if } s = r+1.$$

Therefore $a \underset{2}{\sim} a'$ (Theorem 7).

Now the exceptional case is obvious, since

$$a_1 a_2 = a_2^{-1}(a_2 a_1)a_2.$$

Corollary 4: If any two blocks of consecutive factors of a product are interchanged, then the resulting element is ordinarily 2-conjugate to the original product. An exceptional case occurs when the two blocks contain the entire product; i.e.,

$$a_1 \cdots a_n \top a_{k+1} \cdots a_n \; a_1 \cdots a_k.$$

Proof:

Consider each block as one element and the result follows.

An ordinary interchange of elements or blocks will be called an operation of the first type. The exceptional interchange (involving every factor) will be called an operation of the second type.

Theorem 15: If we apply k operations of the first type and 1 operation of the second type on a product $a = a_1 \cdots a_n$, then the resulting product a' is $(2k+1)$-conjugate to a. But if we apply k operations of the first type, then the resulting product a" is 2k-conjugate to a.

Proof:

Use Theorem 14 and the Converse of Theorem 7.

Before proving the next main theorem; namely, how the product $a_1^k \cdots a_n^k$ is related to $(a_1 \cdots a_n)^k$ and $(a_n \cdots a_1)^k$, we prove it for the case n = 2 in different ways from those given in Theorems 10a, 10b.

Theorem 16a: $(ab)^n \underset{n}{\sim} a^n b^n$ or $(ab)^n \underset{n-1}{\sim} a^n b^n$ according as n is even or odd.

Proof:

Elements in a product are counted from left to right.

Notice that $(ab)^n = (ab)(ab)(ab).....(ab)$,

(1) Interchange the first b with the third a, and the result will be $a^3 b^3 (ab)^{n-3}$.

(2) Interchange the resulting b^3 with the fifth a which will give $a^5 b^5 (ab)^{n-5}$.

(3) Repeat the procedure similarly always replacing the resulting b^k with the $(k+2)$th a.

(4) We notice that if n is odd, we will need $\frac{n-1}{2}$ operations of the first type to give us $a^n b^n$.

Therefore

$$(ab)^n \underset{n-1}{\sim} a^n b^n \quad \text{(Theorem 15)}.$$

(4') But if n is even, then after $\frac{n-2}{2}$ operations (of the first type) the result will be $a^{n-1} b^{n-1} ab$. Now interchange b^{n-1} with the last a, (another operation of the first type), then the result will be $a^n b^n$.

Therefore $(ab)^n \underset{n}{\sim} a^n b^n$ (since $n = 2(\frac{n-2}{2}) + 2.1$, and apply Theorem 15) and the result follows from (4) and (4').

Notice that all the operations are of the first type, (this will be used later).

Theorem 16b: $(ab)^n \underset{n}{\sim} b^n a^n$

Proof:

$$(ab)^n = (ab)(ab)(ab).....(ab).$$

(1) Repeat the procedures (1),(2),(3) that are in theorem 16a.

(2) If n is odd then after $\frac{n-1}{2}$ operations (first type) we will get $a^n b^n$., now interchange a^n and b^n (second type operation), and the result will be $b^n a^n$.

Therefore $(ab)^n \underset{n}{\sim} b^n a^n$ (Theorem 15 and the fact $2(\frac{n-1}{2})+1.1=n$).

(2') If n is even, then after $\frac{n-2}{2}$ operations (first type) we will get $a^{n-1} b^{n-1}$ ab. Now interchange a^{n-1} with the last b (first type operation) which will give us $b^n a^n$.

Therefore $(ab)^n \underset{n}{\sim} b^n a^n$ (Theorem 15 and the fact $2(\frac{n-2}{2})+2.1 = n$) and the result follows from (2) and (2').

Theorem 17a: $(a_1 \ldots a_m)^n \overbrace{\qquad}^{(m-1)(n-1)+1} a_1^n \ldots . a_m^n$ if both m,n are even; otherwise

$$(a_1 \ldots . a_n)^n \overbrace{\qquad}^{(m-1)(n-1)} a_1^n \ldots . a_m^n .$$

Proof:

$$(a_1 \ldots . a_m)^n = (a_1 \ldots . a_m)(a_1 \ldots . a_m) \ldots . (a_1 \ldots . a_m).$$

(1) Move all products $(a_{m-1}\ a_m)$, except the last one, successively to the position immediately after the last a_{m-1}. (After each step there is a new a_{m-1} in the last position).

(2) This will require (n-1) operations (first type) to write

$$(a_1 \ldots . a_{m-2})^n\ a_{m-1}^n\ a_m^n .$$

(3) We repeat, similarly, the procedure for $a_{m-3}\ a_{m-2}$ and then for successive pairs, always needing (n-1) operations for that.

(4) If m is odd, we notice that we need $(\frac{m-1}{2})(n-1)$ operations (first type) to write $(a_1 \ldots . a_m)^n$ as $a_1^n\ a_2^n \ldots . \ a_m^n$ irrespective of n being odd or even.

Therefore $(a_1 \ldots . a_m)^n \underbrace{\qquad\qquad}_{(m-1)(n-1)} a_1^n \ldots . \ a_m^n$.

(5) If m is even we will need $(\frac{m-2}{2})(n-1)$ operations (first type) to write $(a_1 \ldots . a_m)^n$ as $(a_1 a_2)^n\ a_3^n \ldots . \ a_m^n$, and to get the desired product $a_1^n \ldots . \ a_m^n$, we should now differentiate between n being odd or even.

If n is odd we need another $\frac{n-1}{2}$ operations (first type) (Theorem 16a) to change $(a_1 a_2)^n$ to $a_1^n\ a_2^n$;

i.e., the sum of all operations is $(\frac{m-2}{2})(n-1) + \frac{n-1}{2}$.

If n is even, then we need another $\frac{n}{2}$ operations (first type) (see Theorem 16a) to interchange $(a_1 a_2)^n$ to $a_1^n\ a_2^n$;

i.e., the sum of all operations is $(\frac{m-2}{2})(n-1) + \frac{n}{2}$.

Therefore $(a_1 \ldots . a_m)^n \underbrace{\qquad\qquad}_{(m-1)(n-1)} a_1^m \ldots . a_m^n$, if n is odd, m even,

or

$(a_1 \ldots . a_m)^n \underbrace{\qquad\qquad\qquad}_{(m-1)(n-1)+1} a_1^m \ldots . a_m^n$, if n is odd, m even.

Hence the theorem follows from (4) and (5).

<u>Theorem 17b:</u> $(a_1 \ldots . \ a_m)^n \underbrace{\qquad}_{(m-1)_n} a_m^n \ldots . \ a_1^n$.

Proof:

Case 1: m and n are not both even

$(a_1 \ldots . a_m)^n \underbrace{\qquad\qquad}_{(m-1)(n-1)} a_1^n \ldots . a_m^n$ (Theorem 17a),

and

$a_1^n \ldots . a_m^n \underbrace{\qquad}_{m-1} a_m^n \ldots . \ a_1^n$ (Theorem 6).

Therefore

$(a_1 \ldots . a_m)^n \underbrace{\qquad\qquad}_{(m-1)(n)} a_1^n \ldots . \ a_m^n$ (Theorem 12).

Hence the theorem is true in this case.

Case 2: n is even.

Consider

$$(a_1....a_m)^n = (a_1....a_m)(a_1....a_m)(a_1....a_m).....(a_1....a_m).$$

(1) Interchange the first product $a_1....a_{m-1}$ with the 2nd a_m whichl will give us $a_m^2(a_1....a_{m-1})^3\ (a_1....a_{m-1})^{n-3}$.

(2) Interchange $(a_1....a_{m-1})^3$ with the 4th a_m which will give us $a_m^4(a_1....a_{m-1})^5\ a_m\ (a_1....a_{m-1})^{n-5}$.

(3) Repeat the same procedure always interchanging the resulting $(a_1....a_{m-1})^k$ with the (k 1)th a_m.

(4) Since n is even, we will need $\frac{n}{2}$ operations (first type) to get $a_m^n(a_1....a_{m-1})^n$.

(5) We repeat the above four procedures, similarly, for pushing any one of a_{m-1}^n, a_{m-2}^n,...,a_2^n to its palce in the product $a_m^n....a_1^n$, and in every time using $\frac{n}{2}$ operations (first type) for that.

I.e., the sum of all operations needed to change $(a_1...a_m)^n$ to $a_m^n....a_1^n$ is $(m-1)(\frac{n}{2})$ operations.

Therefore

$$(a_1....a_m)^n \overbrace{\quad\quad}^{(m-1)n} a_m^n .... a_1^n, \text{ n is even.}$$

In the theorems just proved, it may be possible to reduce the order of conjugacy, because we may prove $y \widetilde{k} x$ without disproving $y \widetilde{k-1} x$. For some theorems there may be special values of m,n or k for which a reduction in the order of conjugacy is possible. Or, some investigator may in future find that the order may be reduced even in a general theorem.

CHAPTER IV

SOME APPLICATIONS OF k-CONJUGACY

Definition 12: A one-to-one correspondence of any set S with itself is called a permutation. If permutations p and q are performed successively on S, then the resulting permutation is called the product of p and q, denoted by pq.

If the elements of S are $a_1, a_2, \ldots, a_n$ (when it is convenient, a_i may be replaced by $i (i = 1,2,\ldots,n)$), then any permutation may be represented as $\begin{pmatrix} a_1 \ldots a_n \\ a'_1 \ldots a'_n \end{pmatrix}$ or $a_i \rightarrow a'_i$. Every element in the first row is replaced by the element under it, the elements $a'_1, \ldots, a'_n$ being the elements of S in some order. For example; let S consists of the letters a,b,c,d,e; then $\begin{pmatrix} a & b & c & d & e \\ d & c & e & a & b \end{pmatrix}$ means $a \rightarrow d$, $b \rightarrow c$, $c \rightarrow e$, $d \rightarrow a$ and $e \rightarrow b$. It may also be written as (ad)(bce) which means that a and d are permuted in a 2-cycle disjointly from b,c and e that are permuted in a 3-cycle.

To see what is meant by the product, consider $p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$ and $q = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$, then $pq = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$ and $qp = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$ or we see it this way $p = (1\ 4\ 2\ 3)$ and $q = (1\ 2\ 4\ 3)$, $pq = (1\ 3\ 2)$ and $qp = (1\ 3\ 4)$.

Theorem 18: The permutations of S form a group under the operation defined above.

Proof: see [2, p. 64].

Definition 13: If S is a finite set of n elements, the group S_n of all its permutations is called the symmetric group of degree n. Its order is n!

Lemma 3: Every finite permutation can be uniquely resolved into cycles which operate on mutually exclusive sets of objects; i.e., it can be represented as a product of disjoint cycles.

Proof: See [2, p. 66].

Theorem 19: S_n is generated by its 2-cycles and even by the 2-cycles (12)(13),...(1n), (designating the permuted objects by 1,2,...,n).

Proof:

Every k-cycle is a product of (k-1) 2-cycles, namely (1 2 ...k) = (12) (13)...(1k) and every 2-cycle (ij)(i≠ 1, j ≠ 1) may be written as the product (1i)(1j)(1i).

Theorem 20: If x and a are any two permutations (elements) in S_n, then a^{-1} xa is the result of applying the permutation a to the cycles of x (not multiplication of x by a), and consequently x and a^{-1} xa have the same cycle structure.

Proof:

Suppose x changes i into j,

and a changes i into k and j into m;

then a^{-1} changes k into i and m into j,

and a^{-1} xa changes k into m.

Therefore $i \rightarrow j$ is replaced by $k \rightarrow m$;

e.g. let $x = (13)(245)$ and $a = (235)$; then

$$a^{-1} xa = (532)(13)(245)(235) = (15)(342).$$

Corollary 5: Two permutations in S_n are conjugate if and only if they have the same cycle structure.

Proof: See [2, p. 71].

Definition 14: A permutation of 1,2,...n is even if it leaves the product $\prod_{i<j} (x_i - x_j)$ fixed, but odd if it changes the sign. It follows immediately that the product of two even permutations or two odd permutation is even, while the product of an odd permutation and an even permutation is odd.

Theorem 21: In any group of permutations G either all or exactly half the permutations are even; the even permutations of G from a group by themselves.

Proof: See [2, p.77].

Definition 15: The set of all even permutations in S_n form a subgroup called the alternating group A_n, of degree n and of order $\frac{1}{2}n!$

Theorem 22: A 2-cycle is odd

Proof: See [2, p.75].

Corollary 6: A k-cycle is even (odd) if k is odd (even).

Proof:

Any k-cycle may be written as a product of (k-1) 2-cycles(proof

of Theorem 18). Each 2-cycle changes the sign of $\prod_{i<j} (x_i - x_j)$, so the k-cycle changes the sign of $\prod_{i<j} (x_i - x_j)$, (k-1) times.

From here on, if k is even (odd), then a k-cycle will be called an odd(even) cycle.

Lemma 4: A permutation expressed as a product of disjoint cycles is even if and only if the number of its odd cycles is even.

Proof:

If the number of the odd cycles in the permutation is even, then it follows that their product is even, (this follows from the fact that these odd cycles change the sign of $\prod_{i<j}(x_i - x_j)$, an even number of times, which implies that its sign is finally unchanged). Therefore the product of all cycles in the permutation is even, and hence the permutation is even. Similarly, it is clear that a permutation containing an odd number of odd cycles is odd.

Lemma 5: A permutation is a commutator if and only if it may be expressed as a product of two permutations having the same cycle structure.

Proof:

a) if p is a commutator, then $p = a^{-1} b^{-1} ab = a^{-1}(b^{-1}ab)$, but a^{-1} and b^{-1} ab have the same cycle structure, since a and b^{-1} ab have the same cycle structur (see Theorem 20) also a and a^{-1} have the same cycle structure.

Therefore p is the product of two permutations having the same cycle structure.

b) If we have the product pq where p and q are two permutations that have the same cycle structure, then we can always find a third permutation r such that

$$p^{-1} = c^{-1} q c \quad \text{(Theorem 20)};$$

therefore

$$q = c p^{-1} c^{-1}$$

and

$$pq = p c p^{-1} c^{-1},$$

which is a commutator.

Lemma 6: Any product of two disjoint odd cycles may be written as a product of two cycles of equal length.

Proof:

Consider the cycles $(a_1,\ldots.a_m)$, $(b_1,\ldots.b_k)$ where $a_i \neq b_j$ for all $i = 1,2,\ldots,m$ and $j = 1,2,\ldots,k$; also m,k are even.

If $m = k$, no further work is necessary. If $m \neq k$, we may assume that $m > k$.

Let $\frac{m+k}{2} = r$.

Then

$$(a_1\ldots.a_m)(b_1\ldots.b_k) = (a_1\ldots.a_r)(a_1a_{r+1}\ldots.a_m)(b_1\ldots b_k)$$

$$= (a_1\ldots.a_r)(a_1a_{r+1}\ldots a_m)(a_{r+1}b_1)(a_{r+1}b_1)(b_1\ldots b_k)$$

$$= (a_1\ldots a_r)(a_1b_1a_{r+1}\ldots a_m)(a_{r+1}b_2\ldots b_kb_1)$$

$$= (a_1\ldots a_r)(a_1b_1)(a_1a_{r+1}\ldots a_m)(a_{r+1}b_2\ldots b_kb_1)$$

$$= (a_1\ldots a_rb_1)(a_1b_2\ldots b_kb_1a_{r+1}\ldots a_m)$$

= the product of two cycles of length $r+1$.

Theorem 23: Every even permutation is a commutator in S_n.

Proof:

Let x be an even permutation expressed as a product of disjoint cycles. We claim that x = ab where a and b are two permutations of the same structure, which implies that x is a commutator. Consider any two successive odd cycles, we can write them as a product of two cycles having the same length (Lemma 6), now move the left one of the resulting cycles to the left extremity of the product x and the other to the right extremity of x, (this may always be done, since each cycle is permuted only with cycles disjoint from itself). Repeat the same procedure with pairs of consecutive odd cycles, in each case moving the left resulting cycle to the left extremity and the other to the right extremity. Continue until all odd cycles have been dealt with. Then consider every even cycle in the product x, and we write it as the product of two similar cycles, since

$$(a_1 \ldots a_k) = (a_1 a_2 \ldots a_{\frac{k+1}{2}})(a_1\ a_{\frac{k+3}{2}} \ldots a_k)$$

if k is odd, and then move the left one of the resulting cycles to the left extremity and the other to the right extremity. Repeat the same procedure with every even cycle. The result will be x = ab, where a is the product of all cycles moved to the left, and b is the product of all cycles moved to the right. Thus a and b have the same cycle structure, and consequently x is a commutator.

After this theorem has been proved, I found a proof for it by Ore, [5, pp.307-414].

Definition 15: A group G belongs to conjugacy class k if k is the smallest integer for which k-conjugacy is an equivalence relation separating G into the cosets of C.

From Theorem 8 it is seen that k is even, that each element of C may be written as a product of $\frac{k}{2}$ commutators ($k \geq 2$) or that any two elements in C are k-conjugate.

Theorem 24: If G is abelian, then G belongs to conjugacy class 0; i.e., $k = 0$.

Proof:

If G is abelian, then $ab = ba$ (for all a,b in G); therefore

$$a^{-1} b^{-1} ab = e;$$

i.e., the only element in the commutator subgroup is the identity element e.

But we know that $e \sim_0 e$, therefore the result follows.

Theorem 25: The symmetric group S_n ($n > 2$) belongs to conjugacy class 2.

Proof:

The proof follows from the fact that every even permutation is a commutator and that the commutator subgroup is the alternating group.

Theorem 26: The dihedral group D_n defined by the set of generators $\{a,b\}$ with the relations $a^2 = b^n = (ab)^2 = e$ belongs to conjugacy class 2:

To prove this theorem, we introduce a Lemma.

Lemma 6: The commutator subgroup C of D_n is the subgroup generated by b^2, and the order of C is either n or $\frac{n}{2}$ according as n is odd or even.

To prove this, we note that abab = e, then $ab = b^{-1} a^{-1} = b^{-1}a$; i.e., if a is to the left of b and we move it to the right of b, then we change b to b^{-1}.

Now consider the general form of a commutator in D_n which is

$$c = (a^i b^j)^{-1} (a^k b^\ell)^{-1} (a^i b^j)(a^k b^\ell)$$

where

$$i,k = 0,1 \quad \text{and} \quad \ell,\ j = 0,1,\ldots,n-1$$

i.e.;

$$c = b^{-j} a^{-i} b^{-\ell} a^{-k} a^i b^j a^k b^\ell,$$

and let us consider the four cases

a) $i = 0,\ k = 0$

b) $i = 1,\ k = 0$

c) $i = 0,\ k = 1$

d) $i = 1,\ k = 1$

a) $c = b^{-j} a^0 b^{-\ell} a^0 b^j a^0 b^\ell = b^{-j-\ell+j+\ell} = b^0$

b) $c = b^{-j} a^{-1} b^{-\ell} a\, b^j b^\ell$

$= b^{-j} a\, a\, b^\ell\ b^j b^\ell$ since $a = a^{-1}$ and $b^{-\ell} a = ab^\ell$

$= b^{-j} b^\ell\ b^j b^\ell$ since $a^2 = e$

$= b^{2\ell}$

c) $c = b^{-j} b^{-\ell} a^{-1} b^{j} ab^{\ell}$

$= b^{-j} b^{-\ell} a b^{j} a b^{\ell}$ since $a^{-1} = a$

$= b^{-j} b^{-\ell} a^{2} b^{-j} b^{\ell}$ since $b^{j}a = ab^{-j}$

$= b^{-j} b^{-\ell} b^{-j} b^{\ell}$ since $a^{2} = e$

$= b^{-2j}$

d) $c = b^{-j} a b^{-\ell} a^{-1} a b^{j} a b^{\ell}$

$= b^{-j} a b^{-\ell} b^{j} a b^{\ell}$ since $a^{-1} a = e$

$= b^{-j} a^{2} b^{\ell} b^{-j} b^{\ell}$ since $b^{j}a = ab^{-j}$ and $b^{-\ell}a = ab^{\ell}$

$= b^{-j} b^{\ell} b^{-j} b^{\ell}$ since $a^{2} = e$

$= b^{2(\ell - j)}$

We notice that the commutator subgroup consists of elements that are even powers of b. In fact, it contains every even power, because j and ℓ assume independently all values from 0 to n-1. If n is odd then $\{b^2\} = \{b\}$, i.e.; the order of C is n, and if n is even, then the order of C is $\frac{n}{2}$, since $\{b^2\}$ contains half of $\{b\}$ which is of order n.

Proof of theorem 26:

Any element in C which is in the form b^{2r} can be written as $a^{-1} b^{-r} ab^{r}$ which is a commutator, and any element in the form b^{2r+1} (this happens if n is odd), is written as

$$b^{2r+1} = b^{2r+1+n}, \text{ since } b^n = 1$$

$$= a^{-1} b^{-\frac{2r+1+n}{2}} \; a \; b^{\frac{2r+1+n}{2}} \quad \text{(notice that } \frac{2r+1+n}{2} \text{ is an integer)}$$

$$= \text{commutator.}$$

Therefore, we can express each element in the commutator subgroup as a commutator hence k = 2 in this group.

Theorem 27: The group generated by the following permutations, (ac)(eg)(ik), (ab)(cd)(mO),(ef)(gh)(mn)(Op), (ij)(kl), belongs to conjugacy class 4.

Proof:

According to Carmichael [3, p.39, Ex. 30], the commutator subgroup of this group contains just one element which is not a commutator, namely (ik)(jl)(mO)(np). Since this element is the product of two commutators (ik)(jl) and (mO)(np), k = 4 in this group.

REFERENCES

1. Yff, P., On k-Conjugacy in a Group, Proceedings of the Edinburgh Mathematical Society, vol. 14(series II), part 1, June 1964.

2. Ledermann, W., Introduction to the Theory of Finite Groups. Oliver and Boyd, Edinburgh and London, New York; 1961.

3. Carmicheal, R.D., Introduction to the Theory of Groups of Finite order. Ginn and Company, Boston, London, 1937.

4. Burnside, W., Theory of Groups of Finite Order, 2nd ed., Dover publications Inc. 1955.

5. Ore, Oystein, Some Remarks on Commutators, American Mathematical Society, vol. 2, 1951, (pp.307-314).