

Group Theory

James D Emery

5/9/2011

Contents

1	Introduction	2
2	Permutation Groups	2
3	The Factorial Expansion of a Number	8
4	Generating Permutations	10
5	Cosets and Normal Subgroups	18
6	Symbols for Common Groups	19
7	Abelian Groups	19
8	Physics and Group Theory	19
9	The Isometries of the Cube	19
10	Symmetry Groups	23
11	A Program to Compute the Isometries of the Cube by Brute Force	24
12	Free Groups	28
13	Actions and Orbits	30

14 The relation between the Lorentz group and $SL(2, C)$	31
15 Symmetry	31
16 Conjugates	31
17 Noether's Theorem	31
18 Bibliography	31

1 Introduction

The theory of groups originated as the study of the roots of polynomial equations. The "group" was the set of roots, in particular it was a set of permutations of these roots. That is, it was what we would now call a permutation group. For a nice outline of the historical classical theories of the roots of equations, see, **Mathematics: Its Content, Methods, and Meaning**, Volume I, pp 255-280, by Aleksandrov, Kolmogorov, Laurent'ev, translated by S H Gould et al. This includes Cardan's formula for the cubic, Lagrange's methods, the Lagrange resolvent, Abel's proof of the impossibility of solving the general equation of the 5th degree and higher by radicals, and a good outline of Galois theory.

A group G is a set with a binary operation. The operation is associative. For a, b , and c in G , $(ab)c = a(bc)$. A group G has an identity element e . For every element g of G , $eg = ge = g$. An element g of G has an inverse g^{-1} . For every element g of G , $gg^{-1} = e$ and $g^{-1}g = e$.

2 Permutation Groups

A permutation is a 1-1 mapping of a finite set to itself. Given a set $S = \{a_1, a_2, \dots, a_n\}$, a permutation ϕ is a map such as

$$\left[\begin{array}{l} a_1 \rightarrow \phi(a_1) \\ a_2 \rightarrow \phi(a_2) \\ \dots \dots \dots \\ a_n \rightarrow \phi(a_n) \end{array} \right]$$

We may abbreviate this display by just writing the sequence of images

$$\phi(a_1)\phi(a_2)\phi(a_3)\dots\phi(a_n)$$

Thus if $S = \{a_1, a_2, \dots, a_5\}$, then $a_2a_3a_1a_5a_4$ means

$$\begin{bmatrix} a_1 & \rightarrow & a_2 \\ a_2 & \rightarrow & a_3 \\ a_3 & \rightarrow & a_1 \\ a_4 & \rightarrow & a_5 \\ a_5 & \rightarrow & a_4 \end{bmatrix}$$

We can further abbreviate the permutation by writing just the indices, and so writing the permutation as 23154. Suppose

$$\phi_1 = 23154$$

and

$$\phi_2 = 41523$$

Then

$$\phi_1 = \begin{bmatrix} 1 & \rightarrow & 2 \\ 2 & \rightarrow & 3 \\ 3 & \rightarrow & 1 \\ 4 & \rightarrow & 5 \\ 5 & \rightarrow & 4 \end{bmatrix}$$

and

$$\phi_2 = \begin{bmatrix} 1 & \rightarrow & 4 \\ 2 & \rightarrow & 1 \\ 3 & \rightarrow & 5 \\ 4 & \rightarrow & 2 \\ 5 & \rightarrow & 3 \end{bmatrix}$$

We can write ϕ_2 in the order

$$\phi_2 = \begin{bmatrix} 2 & \rightarrow & 1 \\ 3 & \rightarrow & 5 \\ 1 & \rightarrow & 4 \\ 5 & \rightarrow & 3 \\ 4 & \rightarrow & 2 \end{bmatrix}$$

Then writing ϕ_1 and ϕ_2 together

$$\begin{bmatrix} 1 & \rightarrow & 2 \\ 2 & \rightarrow & 3 \\ 3 & \rightarrow & 1 \\ 4 & \rightarrow & 5 \\ 5 & \rightarrow & 4 \end{bmatrix} \begin{bmatrix} 2 & \rightarrow & 1 \\ 3 & \rightarrow & 5 \\ 1 & \rightarrow & 4 \\ 5 & \rightarrow & 3 \\ 4 & \rightarrow & 2 \end{bmatrix}$$

We read off immediately that the product $\phi_1\phi_2$ is

$$\begin{bmatrix} 1 & \rightarrow & 1 \\ 2 & \rightarrow & 5 \\ 3 & \rightarrow & 4 \\ 4 & \rightarrow & 3 \\ 5 & \rightarrow & 2 \end{bmatrix}.$$

Function composition is defined as $\phi_2 \circ \phi_1(x) = \phi_2(\phi_1(x))$. We have defined the product of permutations as

$$\phi_1\phi_2(x) = \phi_2 \circ \phi_1(x).$$

So that multiplication and composition are in opposite order. This discrepancy is one of the reasons that some algebra books, such as Herstein's **Topics in Algebra**, define composition in the opposite order. For our example we have $\phi_1\phi_2 = 15432$.

Consider the cycle of a permutation obtained by starting with an element k and listing the mapping sequence

$$(k\phi(k)\phi^2(k)\phi^3(k)\dots\phi^j(k))$$

until we return to the original k . Thus starting with element 3 in ϕ_1 we get the cycle (312) because 3 maps to 1 and 1 maps to 2 and 2 maps to 3. A cycle starting with 5 is (54). A cycle by itself is a permutation if we assume that elements that do not occur in the cycle map to themselves. Thus (312) becomes the permutation

$$\begin{bmatrix} 1 & \rightarrow & 2 \\ 2 & \rightarrow & 3 \\ 3 & \rightarrow & 1 \\ 4 & \rightarrow & 4 \\ 5 & \rightarrow & 5 \end{bmatrix}$$

or 23145. The original permutation ϕ_1 is written as a product of disjoint cycles as

$$\phi_1 = (312)(54)$$

Clearly cycle (123) is the same as (312). So we can write any permutation as a disjoint product of cycles in a canonical form, where the first element of any cycle is the smallest number in the cycle. Thus we may write

$$\phi_1 = (123)(45).$$

Disjoint cycles commute, so we can also list each cycle in the product according to the size of its first element in our canonical form. Thus each permutation may be written uniquely as a product of disjoint cycles. Obviously permutations do not commute in general.

A transposition is a two cycle where two elements are interchanged. A cycle such as (312) may be written as a product of transpositions as

$$(312) = (31)(32).$$

In general one can write

$$(a_1, a_2, a_3, a_4, \dots, a_n) = (a_1, a_2)(a_1, a_3)(a_1, a_4)\dots(a_1, a_n).$$

For example an a_k is mapped to a_1 in the k th cycle and then a_1 is mapped to a_{k+1} in the k th cycle, so the net effect of the product is to map a_k to a_{k+1} . Hence every permutation can be written as a product of transpositions. Such products of transpositions are not necessarily disjoint.

A permutation is called even if it can be written as a product of an even number of transpositions. A permutation is called odd if it can be written as a product of an odd number of transpositions. We shall show that a permutation can not be both even and odd. To this end we define a polynomial $P(x_1, x_2, x_3, \dots, x_n)$ in n variables as

$$P(x_1, \dots, x_n) = \prod_{i < j} (x_i - x_j).$$

Given a permutation ϕ we define the polynomial Q_ϕ by

$$Q_\phi(x_1, \dots, x_n) = P(x_{\phi(1)}, \dots, x_{\phi(n)}).$$

Then if ϕ is a transposition we have

$$Q_\phi = -P.$$

If ϕ is a product of m transpositions, it is an odd permutation and $Q_\phi = -P$ if m is an odd number, and it is an even permutation and $Q_\phi = P$ if m is an even number. So a permutation can't be both odd and even.

A permutation group on n symbols has $n!$ elements. A product of two even permutations is even, the identity is even, and the inverse of an even permutation is clearly even. This later fact is true because the reversing of each transposition gives the inverse. Hence the set of even permutations forms a subgroup. This subgroup is called the alternating group.

If we display the multiplication table of a finite group we see that each row and each column is a permutation of the group symbols. For example consider the group called the four group, which is the symmetry group of the vertices of a rectangle that is not square. Let a coordinate system be centered at the center of a rectangle in the xy plane. The 4 elements of the group are the identity e , rotation α by 180 degrees about the z axis, rotation β by 180 degrees about the y axis, and γ rotation by 180 degrees about the x axis. Then the multiplication table is

*	e	α	β	γ
e	e	α	β	γ
α	α	e	γ	β
β	β	γ	e	α
γ	γ	β	α	e

Let a be the top left hand corner of the rectangle, b the top right hand corner, c the bottom right hand corner and d the bottom left hand corner. Then as vertex permutations we have

$$\alpha = (ad)(bc)$$

$$\beta = (ab)(cd)$$

$$\gamma = (ac)(bd).$$

From this one may compute the products of the table. The lower right 4 by 4 table gives permutations of the group symbols.

Cayley's theorem (Herstein) says that every finite group is a subgroup of the symmetry group on the n symbols of the group. In the example above we can map every element of G to a column of the table in the following way.

$$e \rightarrow e\alpha\beta\gamma$$

$$\alpha \rightarrow \alpha e\gamma\beta$$

$$\beta \rightarrow \beta\gamma e\alpha$$

$$\gamma \rightarrow \gamma\beta\alpha e$$

This is clearly a 1-1 and onto map to the columns of the table. The columns are obtained by multiplication on the right. Let G be a general finite group. We define a mapping H from G to the permutations of the group symbols, namely to the columns in the multiplication table. We define

$$H : g \rightarrow \chi_g,$$

by

$$\chi_g(x) = xg$$

where $x \in G$. Clearly H is 1 to 1. We shall prove that H is a homomorphism. We have

$$H(g_1g_2) = \chi_{g_1g_2}.$$

and

$$\chi_{g_1g_2}(x) = xg_1g_2 = \chi_{g_1}(x)g_2 = \chi_{g_2}(\chi_{g_1}(x)) = \chi_{g_1}\chi_{g_2}(x).$$

Hence

$$H(g_1g_2) = H(g_1)H(g_2)$$

So H is a homomorphism. So G is isomorphic to a subgroup of the permutation group of the symbols of G .

Algorithms for permutations may be found in the program **perm.ftn** and in the library source file **emerylib.ftn**. A reference for computation is **Applied Combinatorial Mathematics** by Beckenbach.

3 The Factorial Expansion of a Number

A positive integer n has a factorial expansion of the form

$$n = a_1 1! + a_2 2! + a_3 3! + \dots + a_k k!,$$

where $0 \leq a_k \leq k$. The numbers $\{a_1, a_2, \dots, a_k\}$ are the factorial digits. Let $n_1 = n$. Dividing n_1 by 2 we have

$$n_1 = 2n_2 + a_1,$$

where a_1 is the remainder after division by 2. And

$$2n_2 = n_1 - a_1 = a_2 2! + a_3 3! + \dots + a_k k!.$$

So

$$n_2 = \frac{a_2 2! + a_3 3! + \dots + a_k k!}{2!}.$$

We shall prove that this may be continued to compute each a_j .

Suppose we define n_j recursively as the quotient obtained by dividing n_{j-1} by j with a remainder less than j . We shall prove by induction that we have for $m = 2, 3, \dots, k$,

$$n_m = (m + 1)n_{m+1} + a_m,$$

where n_{m+1} is the quotient obtained by dividing n_m by $m + 1$, and a_m is the remainder. Further we have

$$n_{m+1} = \frac{a_{m+1}(m + 1)! + \dots + a_k k!}{(m + 1)!}.$$

So suppose these equations are true for $m \leq j$. Then we have

$$\begin{aligned} n_{j+1} &= \frac{a_{j+1}(j + 1)! + \dots + a_k k!}{(j + 1)!} \\ &= a_{j+1} + \frac{a_{j+2}(j + 2)! + \dots + a_k k!}{(j + 1)!} \\ &= a_{j+1} + (j + 2) \frac{a_{j+2}(j + 2)! + \dots + a_k k!}{(j + 2)!} \end{aligned}$$

$$= (j + 2)n_{j+2} + a_{j+1}.$$

where

$$n_{j+2} = \frac{a_{j+2}(j + 2)! + \dots + a_k k!}{(m + 1)!}.$$

Therefore the equations are true for $m = j + 1$, and hence for all m .

The factorial digits of a number $n \geq 0$ are computed recursively with the equations

$$n_1 = n$$

and

$$n_j = (j + 1)n_{j+1} + a_j,$$

for $j = 2, \dots, k$. We stop when $n_{k+1} = 0$. Thus every nonnegative integer n has a unique factorial expansion.

Proposition.

$$\sum_{j=1}^k j(j!) = (k + 1)! - 1.$$

Proof. We have

$$1(1!) = (2!) - 1.$$

Suppose the equation is true for k , then

$$1(1!) + 2(2!) + \dots + k(k!) = (k + 1)! - 1,$$

so

$$\begin{aligned} 1(1!) + 2(2!) + \dots + k(k!) + (k + 1)(k + 1)! &= (k + 1)! - 1 + (k + 1)(k + 1)! \\ &= (k + 1)!(1 + (k + 1)) - 1 = (k + 2)! - 1. \end{aligned}$$

So the equation is true for all integers.

Corollary. Suppose a number a has factorial digits

$$a_1, a_2, \dots$$

and a number b has factorial digits

$$b_1, b_2, \dots$$

Let j be the largest integer such that $a_j \neq b_j$. Then $a > b$ if and only if $a_j > b_j$.

Proof. Suppose $a_j > b_j$. Let $c_j = a_j - b_j$. Then Using the proposition we have

$$c_j j! \geq j! > \sum_{p=1}^{j-1} p(p!) \geq \sum_{p=1}^{j-1} b_p p!$$

Hence

$$\begin{aligned} a &= a_1 1! + a_2 2! + \dots + a_j j! + \dots + a_k k! \\ &= a_1 1! + a_2 2! + \dots + c_j j! + b_j j! + \dots + a_k k! \\ &= a_1 1! + a_2 2! + \dots + c_j j! + b_j j! + \dots + b_k k! \\ &> a_1 1! + a_2 2! + \dots + a_{j-1} (j-1)! + b \\ &\geq b. \end{aligned}$$

So $a > b$.

To prove the only if claim suppose $a > b$ and $a_j < b_j$. Then by using the argument above, we have $b > a$. But this is a contradiction. So $a_j > b_j$.

4 Generating Permutations

The factorial digits of a number $0 \leq n < (k+1)!$ are the unique nonnegative integers a_1, a_2, \dots, a_k so that

$$n = a_1 1! + a_2 2! + a_3 3! + \dots + a_k k!,$$

where $a_j \leq j$. The identity

$$\sum_{j=1}^k j(j!) = (k+1)! - 1.$$

shows that the largest number that may be represented with k factorial digits is $(k+1)! - 1$. So including the number 0, there are $(k+1)!$ numbers that may be represented with k factorial digits. Now there are $(k+1)!$ permutations of the symbols $0, 1, 2, 3, \dots, k$.

So we can create a 1-1 correspondence between the set of k factorial digits and the permutations of $k+1$ symbols. Permutations may be ordered

lexicographically. We shall create a mapping from integers to permutations that preserves order.

Given an integer n such that $0 \leq n < (k + 1)!$ we compute its factorial digits,

$$n = a_1 1! + a_2 2! + a_3 3! + \dots + a_k k!.$$

We shall construct an upper triangular matrix b_{ij} of size $k + 1$ by $k + 1$ so that the permutation corresponding to integer n will appear in the last column. We construct the matrix by setting $b_{11} = 0$ and $b_{ii} = a_{i-1}$. The elements above the main diagonal are generated as follows. The j th column is generated from the $j - 1$ column. For $i > j$ we let

$$b_{ij} = b_{i-1}$$

if $b_{i,j-1} < b_{jj}$, otherwise we let

$$b_{ij} = b_{i-1} + 1.$$

We have a matrix of the form

$$\begin{bmatrix} b_{11} & b_{12} & b_{13} & \dots & b_{1,k+1} \\ & b_{22} & b_{23} & \dots & b_{2,k+1} \\ & & b_{33} & \dots & \dots \\ & & & \dots & \dots \\ & & & & b_{k+1,k+1} \end{bmatrix}$$

Notice that each column will always contain distinct elements. Also notice that each element of a row never decreases and increases by at most 1 as we move to the left. The element on the diagonal of the i th row is a factorial digit and so is less than or equal to $i - 1$. Therefore the last element of the row in the $k + 1$ column is less than or equal to k . It follows that the $k + 1$ column is a permutation of the symbols $0, 1, 2, 3, 4, 5, \dots, k$. Hence the algorithm generates a mapping from integers to permutations. We shall show below that the mapping preserves order and thus is 1-1.

For example let $k = 9$ and $n = 1000000$. The factorial digits are 022152662. The matrix is

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 2 & 2 & 3 & 3 & 3 & 4 \\ & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & 2 & 3 & 4 & 4 & 5 & 5 & 5 & 6 \\ & & & 2 & 3 & 3 & 4 & 4 & 4 & 5 \\ & & & & 1 & 1 & 1 & 1 & 1 & 1 \\ & & & & & 5 & 6 & 7 & 8 & 9 \\ & & & & & & 2 & 2 & 2 & 3 \\ & & & & & & & 6 & 7 & 8 \\ & & & & & & & & 6 & 7 \\ & & & & & & & & & 2 \end{bmatrix}$$

So the permutation corresponding to n is 2783915604.
 As another example let $k = 5$ and $n = 0$. The matrix is

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ & 0 & 1 & 2 & 3 & 4 \\ & & 0 & 1 & 2 & 3 \\ & & & 0 & 1 & 2 \\ & & & & 0 & 1 \\ & & & & & 0 \end{bmatrix}$$

The permutation is 01245, which is the first permutation of the six symbols 0,1,2,3,4,5 in lexicographic order.

Again let $k = 5$ and $n = 6! - 1 = 719$. This number has factorial digits 12345. The matrix is

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 1 & 1 & 1 & 1 \\ & & 2 & 2 & 2 & 2 \\ & & & 3 & 3 & 3 \\ & & & & 4 & 4 \\ & & & & & 5 \end{bmatrix}$$

The permutation is 543210, which is the last permutation of the six symbols 0,1,2,3,4,5 in lexicographic order.

Let us now show that the mapping preserves order. Suppose we have a pair of integers a and b , with $a > b$. Let them have factorial digits a_1, a_2, \dots, a_k

and b_1, b_2, \dots, b_k respectively. There is a largest j so that $a_j > b_j$. Then the two matrices are identical below row $j + 1$. Let the $j + 1$ row of the matrix for a be

$$a_j = x_{j+1}, x_{j+2}, \dots, x_{k+1}$$

and for b be

$$b_j = y_{j+1}, y_{j+2}, \dots, y_{k+1}.$$

We have $x_{j+1} > y_{j+1}$. Let us consider the next elements of the rows. There are two cases. Case 1: suppose $y_{j+1} \geq b_{j+2, j+2}$, then $y_{j+2} = y_{j+1} + 1$. In this case we have also that $x_{j+1} \geq b_{j+2, j+2}$ so that $x_{j+2} = x_{j+1} + 1$. It follows that $x_{j+2} > y_{j+2}$. Case 2: suppose $y_{j+1} < b_{j+2, j+2}$, then $y_{j+2} = y_{j+1}$. Then since an element of a row never decreases, we must have $x_{j+2} \geq x_{j+1}$. It follows in this case also that $x_{j+2} > y_{j+2}$. Repeating this argument for succeeding elements we find that $x_{k+1} > y_{k+1}$, and so the permutation $\sigma(a) > \sigma(b)$ with the lexicographic order. So order is preserved. Therefore the mapping constructed with this algorithm is 1-1. This algorithm is the lexicographical method of D. N. Lehmer. See Beckenbach.

Given a permutation on $k + 1$ symbols, we can place it in the last column of a $k + 1$ by $k + 1$ matrix b and fill in the preceding columns to get the factorial digits of the permutation number.

Thus if a_1, a_2, \dots, a_{k+1} is the permutation we let

$$b(i, k + 1) = a_{k+2-i}$$

for $i = 1, \dots, k + 1$. Then

let

$$b(i, j) = b(i, j + 1)$$

if $b(i, j + 1) < b(j + 1, j + 1)$ and

$$b(i, j) = b(i, j + 1) - 1$$

if $b(i, j + 1) > b(j + 1, j + 1)$, for $j = 2, \dots, k$ and $i = 1, \dots, k$. Then

$$n = b(2, 2)1! + b(3, 3)2! + b(3, 3)3! + \dots + b(k + 1, k + 1)k!.$$

These computations are implemented in subroutines **perm** and **perminv**.

The Fortran subroutines use this algorithm to return the permutation of the symbols 1,2,3,...,numsym, rather than a permutation of the symbols 0,1,2,3,...,numsym-1. The first permutation number is 1 rather than 0.

Here is a listing:

```

c+ perm    kth permutation in the lexicographic ordering
          subroutine perm(k,numsym,sigma)
c    Input:
c    k      The number of this permutation in the lexicographic
c           ordering. 1 <= k <= numsym!
c    numsym The number of permutation symbols and the
c           length of sigma, numsym < 20
c    Output:
c    sigma  An integer array containing a permutation of the
c           symbols 1,2,3,...,numsym
c
c    The kth permutation of the first numsym positive integers is
c    returned in the array sigma. When k = 1 it returns
c    sigma = 1 2 3 4 ... numsym,
c    when k = numsym! it returns
c    sigma = numsym ..... 4 3 2 1.
c
c    Factorial digits are used for the calculation.
c    numsym should be <= 20
c    This is the lexicographic method of D N Lehmer.
c    Reference: Applied Combinatorial Mathematics,
c    Edwin Beckenbach, Wiley 1964
c    Also see Group Theory, by James Emery, (groups.tex)
c    The method exploits the 1-1 correspondence of factorial
c    digits of numbers < n! -1 and the permutations of n symbols.
c    Starting with the factorial digits, a triangular table is built
c    with the last column a permutation. This is done in such a manner that
c    the mapping from the number to the permutation is monotonic
c    and hence 1-1.
c    See subroutine perminv, which calculates k from sigma.
c    See also subroutine nextperm, which will be more efficient if the whole
c    list of permutations is to be generated.

```

```

integer sigma(*)
dimension nr(20,20),nfdg(40)
m1=numsym-1
itest=0
if(itest .eq. 1)then
  do i=1,numsym
    do j=1,numsym
      nr(i,j)=-1
    enddo
  enddo
endif
call facdig(k-1,nfdg,1,numdg)
if(numdg .ne. m1)then
  k1=numdg+1
  do j1=k1,m1
    nfdg(j1)=0
  enddo
endif
c   write(*,'(1x,10(i2,1x))')(nfdg(i),i=1,numdg)
nr(1,1)=0
do j=2,numsym
  nr(j,j)=nfdg(j-1)
  n2=j-1
  do i=1,n2
    nr(i,j)=nr(i,n2)
    if(nr(i,j).ge.nr(j,j))nr(i,j)=nr(i,j)+1
  enddo
enddo
if(itest .eq. 1)then
  do i=1,numsym
    write(*,'(1x,20(i2,1x))')(nr(i,j),j=1,numsym)
  enddo
endif

do i=1,numsym
  nr(i,numsym)=nr(i,numsym)+1
enddo

```

```

do m=1,numsym
  sigma(numsym+1-m)=nr(m,numsym)
enddo
end

c+ perminv  the number k corresponding to a permutation
           subroutine perminv(numsym,sigma,k)
c   Input:
c   numsym  the number of permutation symbols and the
c           length of sigma
c   sigma   an integer array containing a permutation of the
c           symbols 1,2,3,...,numsym
c   Output:
c   k       the number of this permutation in the lexicographic
c           ordering.
c
c   This is the inverse of the computation performed
c   in subroutine perm.
c   When sigma = 1 2 3 4 ... numsym,
c   it returns k = 1.
c   When sigma = numsym ..... 4 3 2 1,
c   It returns k = numsym!
c
c   This is the inverse for the lexicographic method of D N Lehmer.
c   Reference: Applied Combinatorial Mathematics,
c   Edwin Beckenbach, Wiley 1964
c   The method exploits the 1-1 correspondence of factorial
c   digits of numbers  $< n! - 1$  and the permutations of n symbols.
c   See subroutine perm.
integer sigma(*)
integer b(20,20),nfdg(40)
numdg=numsym-1

itest=0
if(itest .eq. 1)then
  do i=1,numsym
    do j=1,numsym

```

```

        b(i,j)=-1
    enddo
enddo
endif
do j=1,numsym
    b(j,numsym)=sigma(numsym+1-j)-1
enddo
nfdg(numdg)=b(numsym,numsym)
do j=numdg,2,-1
    d=b(j+1,j+1)
    do i=1,j
        if(b(i,j+1) .gt. d)then
            b(i,j)=b(i,j+1)-1
        else
            b(i,j)=b(i,j+1)
        endif
    enddo
    nfdg(j-1)=b(j,j)
enddo
if(itest .eq. 1)then
    do i=1,numsym
        write(*,'(1x,20(i2,1x))')(b(i,j),j=1,numsym)
    enddo
endif
ncode=0
call facdig(n,nfdg,ncode,numdg)
k=n+1
return
end

```

c+ facdig factorial expansion of a number.
subroutine facdig(n,nfdg,ncode,numdg)
dimension nfdg(20)
c this subroutine constructs the factorial digits of n and places
c them in nfdg. numdg is the number of factorial digits.
c if ncode=1 the factorial digits are calculated from n, otherwise
c n is calculated from the factorial digits, which must be supplied

```

c      n= a_1 1! + a_2 2! + ... + a_k k! where 0 <= a_i <= i
      if(ncode .eq. 1)then
          j=n
          m=1
          k=0
          l=1
          do while(l .ne. 0)
              m=m+1
              k=k+1
              l=j/m
              nr=j-l*m
              nfdg(k)=nr
              j=l
          enddo
          numdg=k
          return
      else
          n=0
c      The following computation could be changed to be efficient by
c      reversing the algorithm above.
          do i=1,numdg
              n=n+nfdg(i)*nfac(i)
          enddo
      endif
      return
      end

```

5 Cosets and Normal Subgroups

A left coset of a subgroup H of G is the set gH , where $g \in G$. A right coset of a subgroup H of G is the set Hg . The mapping from H to its left coset gH given by $h \rightarrow gh$ is onto and 1 to 1. Hence all cosets have the same number of elements. The cosets partition the group, thus the order of a subgroup divides the order of the group (Lagranges Theorem). A normal subgroup N has the property that the left cosets equal the right cosets. If N is a normal

subgroup, then the factor group G/N exists. The kernel of a homomorphism is a normal subgroup. If N is the kernel of a homomorphism h then G/N is isomorphic to the image group $h(G)$. The alternating group is a normal subgroup of a permutation group.

6 Symbols for Common Groups

C_n , rotations of the regular n polygon.

D_n , symmetries of the the regular n polygon.

S_n , permutations of the vertices of the n polygon.

$O(n)$, orthogonal matrices.

$SO(n)$, special orthogonal matrices with determinant $+1$.

$U(n)$, unitary matrices.

$SU(n)$, unitary matrices with determinant 1 .

$SL(n, C)$ n by n complex matrices with determinant 1 , complex special linear group.

$GL(n, R)$ real invertible n by n matrices, real general linear group.

7 Abelian Groups

An Abelian group is a group that commutes, so that

$$g_1 + g_2 = g_2 + g_1.$$

The additive symbol $+$ is often used as the operator for Abelian groups.

8 Physics and Group Theory

See the reference **Group Theory and Physics**.

9 The Isometries of the Cube

Let the x, y, z coordinates of the eight vertices of the unit cube be given in order as

```
0 0 0
1 0 0
1 1 0
0 1 0
0 0 1
1 0 1
1 1 1
0 1 1
```

This points are labeled from 0 to 7. The isometries of the cube may be computed by finding all permutations of the eight vertices and retaining those that preserve all distances between vertex pairs. The 48 isometries of the cube are (see `isomcube.ftn`):

```
1 76234510 v=-1
2 56741230 v=-1
3 56214730 v=1
4 26731540 v=1
5 26513740 v=-1
6 67452301 v=-1
7 67325401 v=1
8 47650321 v=1
9 47305621 v=-1
10 37620451 v=-1
11 37402651 v=1
12 74563012 v=-1
13 74036512 v=1
14 54761032 v=1
15 54016732 v=-1
16 04731562 v=-1
17 04513762 v=1
18 65472103 v=1
19 65127403 v=-1
20 45670123 v=-1
21 45107623 v=1
22 15620473 v=1
23 15402673 v=-1
```

24 62375104 v=-1
25 62157304 v=1
26 32670154 v=1
27 32107654 v=-1
28 12650374 v=-1
29 12305674 v=1
30 73264015 v=1
31 73046215 v=-1
32 23761045 v=-1
33 23016745 v=1
34 03741265 v=1
35 03214765 v=-1
36 40375126 v=1
37 40157326 v=-1
38 30472156 v=-1
39 30127456 v=1
40 10452376 v=1
41 10325476 v=-1
42 51264037 v=-1
43 51046237 v=1
44 21563047 v=1
45 21036547 v=-1
46 01543267 v=-1
47 01234567 v=1
48 76543210 v=1

The 24 proper orientation preserving isometries have positive volume element. They are:

1 56214730
2 26731540
3 67325401
4 47650321
5 37402651
6 74036512
7 54761032
8 04513762

9 65472103
 10 45107623
 11 15620473
 12 62157304
 13 32670154
 14 12305674
 15 73264015
 16 23016745
 17 03741265
 18 40375126
 19 30127456
 20 10452376
 21 51046237
 22 21563047
 23 01234567
 24 76543210

The orientation preserving propriety of the isometries can be determined by computing the volume from the faces, or by looking for normal reversal. For example, the first permutation takes face (1 2 3 4) to face (8 7 3 4). The normal of face (1 2 3 4) points in. The normal of face (8 7 3 4) points out. Therefore the isometry is improper.

Let v_{ij} be the vector from point i to point j . Then the volume of the cube is

$$V = v_{12} \cdot v_{14} \times v_{15} = 1.$$

The volume of the isometry σ is

$$V_\sigma = v_{\sigma(1)\sigma(2)} \cdot v_{\sigma(1)\sigma(4)} \times v_{\sigma(1)\sigma(5)}.$$

If V_σ is positive (equal to 1), then the isometry is proper.

We can determine the 24 proper isometries directly. The group of isometries of the cube is a subgroup of the group of all isometries in 3 space. Since the center of the cube is fixed, the isometries of the cube are a subgroup of rotations. Each such rotation has an axis. The cube has three 4-fold rotation axes through the center of faces. This gives $9 = 3(\text{axes}) \times 3(\text{rotations})$ elements of the cubical group. There are four 3-fold axis through space diagonals of the cube. This gives $8 = 4(\text{axes}) \times 2(\text{rotations})$ elements of the cubical group.

There are six 2-fold axis through opposite pairs of edges cube. This gives $6 = 6(\text{axes}) \times 1(\text{rotation})$ elements of the cubical group. The identity is in the group. Thus there are

$$24 = 9 + 8 + 6 + 1,$$

elements of the group.

Any other element must have a different rotation axis of the cube. But there are none. These 24 isometries are all of the proper isometries of the cube.

Another characterization of the proper isometries comes from considering a cube with vertices whose coordinates take values ± 1 . Letting (x, y, z) be the coordinates of a vertex, the mapping of an isometry takes the form $(x, y, z) \rightarrow (u, v, w)$, where each of u, v, w is one of $\pm x, \pm y, \pm z$. For example, consider $(x, y, z) \rightarrow (-x, y, -z)$. This is a rotation about the y axis by 180 degrees. Each such transformation is represented by a matrix. Each element of the matrix has values ± 1 . Each row must have only one nonzero element, otherwise we may find a vertex mapped to a nonvertex. Thus there are eight ways of assigning the plus and minuses so that $(u, v, w) = (\pm x, \pm y, \pm z)$ the x, y, z can be rearranged in 6 ways, hence there are 48 such transformations, 24 proper and 24 nonproper. See section 1.5 in **Group Theory and Physics**.

10 Symmetry Groups

Baumslag lists all finite groups of order less than 16. The Dihedral group D_n is the symmetry group of a regular polygon with n sides. A symmetry group of a polygon is either a cyclic group, or a dihedral group.

The tetrahedral group has 24 elements, the hexahedral group (cube) has 48 elements, the octahedral group has 48 elements (the octahedron is the dual of the hexahedron). The icosahedral group has 120 elements and the dodecahedral group has 120 elements (the icosahedron is the dual of the dodecahedron).

11 A Program to Compute the Isometries of the Cube by Brute Force

```
c isomcube.ftn isometries of the cube 3/23/94
  implicit integer(a-z)
  real*8 dotpr
  dimension p(20)
  dimension x(8)
  dimension y(8)
  dimension z(8)
  real*8 v1(3),v2(3),v3(3),u(3)
  data x/0,1,1,0,0,1,1,0/
  data y/0,0,1,1,0,0,1,1/
  data z/0,0,0,0,1,1,1,1/
  ns=8
  write(*,*)' n! = ',nfac(ns)
  m=nfac(ns)
  mm=0
  do 10 k=1,m
    call perm(k,ns,p)
    do 20 i=1,ns-1
      xi=x(i)
      yi=y(i)
      zi=z(i)
      xpi=x(p(i))
      ypi=y(p(i))
      zpi=z(p(i))
      do 30 j=i+1,ns
        xj=x(j)
        yj=y(j)
        zj=z(j)
        xpj=x(p(j))
        ypj=y(p(j))
        zpj=z(p(j))
        d1=(xi-xj)**2+(yi-yj)**2+(zi-zj)**2
        d2=(xpi-xpj)**2+(ypi-ypj)**2+(zpi-zpj)**2
```

```

        if(d1 .ne. d2)then
            go to 10
        endif
30    continue
20    continue
        mm=mm+1
        v1(1)=x(p(2))-x(p(1))
        v1(2)=y(p(2))-y(p(1))
        v1(3)=z(p(2))-z(p(1))
        v2(1)=x(p(4))-x(p(1))
        v2(2)=y(p(4))-y(p(1))
        v2(3)=z(p(4))-z(p(1))
        v3(1)=x(p(5))-x(p(1))
        v3(2)=y(p(5))-y(p(1))
        v3(3)=z(p(5))-z(p(1))
        call crsspr(v2,v3,u)
        vol=dotpr(v1,u)
        write(*,'(i8,i5,1x,8i1,a,i2)')k,mm,(p(j)-1,j=1,ns),' v=',vol
10    continue
        end
c+ psign sign of permutation.
        subroutine psign(iper,numsym,nsign)
c    sign of permutation ip on numsym symbols
c    sign returned in nsign.
        dimension ip(10),iper(10)
        do 5 i2=1,numsym
5    ip(i2)=iper(i2)
        nsign=1
        l=numsym-1
        do 20 i=1,l
            k=i+1
            do 10 j=k,numsym
                if(ip(i).lt.ip(j))go to 10
            ns=ip(j)
            ip(j)=ip(i)
            ip(i)=ns
            nsign=-1*nsign

```

```

10 continue
20 continue
   return
   end
c+ perm      permutations.
   subroutine perm(k,numsym,sigma)
c   the k th permutation of the first numsymb positive integers is
c   returned in the 1 dimensional array sigma.  ndim is the dimension
c   of sigma.  uses factorial digits to calculate the
c   numsymb should be .le. 10
c   sigma is an integer variable
   integer sigma(*)
   dimension nr(10,10),nfdg(20)
   m1=numsym-1
   call facdig(k,nfdg,1,numdg)
c   print 110,k,(nfdg(m),m=1,numdg)
   if(numdg.eq.m1)go to 40
   k1=numdg+1
   do 30 j1=k1,m1
30  nfdg(j1)=0
40  nr(1,1)=0
   do 90 j=2,numsym
   nr(j,j)=nfdg(j-1)
   n2=j-1
   do 80 i=1,n2
   nr(i,j)=nr(i,n2)
   if(nr(i,j).ge.nr(j,j))nr(i,j)=nr(i,j)+1
80  continue
90  continue
   do 100 i=1,numsym
100 nr(i,numsym)=nr(i,numsym)+1
   do 110 m=1,numsym
110 sigma(m)=nr(m,numsym)
   end
c+ facdig    factorial expansion of a number.
   subroutine facdig(n,nfdg,ncode,numdg)
   dimension nfdg(20)

```

```

c      this subroutine constructs the factorial digits of n and places
c      them in nfdg. numdg is the number of factorial digits.
c      if ncode=1 the factorial digits are calculated from n, otherwise
c      n is calculated from the factorial digits, which must be supplied
      if(ncode.ne.1)go to 20
      j=n
      m=1
      k=0
10  m=m+1
      k=k+1
      l=j/m
      nr=j-l*m
c      j=m*l+nr
      nfdg(k)=nr
      j=1
      if(l.ne.0)go to 10
      numdg=k
      return
20  do 50 i=1,numdg
50  n=nfdg(i)*nfac(i)
      return
      end
c+ nfac      factorial.
      function nfac(n)
c      n factorial.
      i=1
      do 20 k=2,n
20  i=i*k
      nfac=i
      return
      end
c+ dotpr      scalar product.
      function dotpr(a,b)
      implicit real*8(a-h,o-z)
      dimension a(3),b(3)
      s=0.
      do 10 i=1,3

```

```

10  s=s+a(i)*b(i)
    dotpr=s
    return
    end
c+ crsspr  vector cross product.
    subroutine crsspr(a,b,c)
    implicit real*8(a-h,o-z)
c    c=product of a and b
    dimension a(3),b(3),c(3)
    c(1)=a(2)*b(3)-a(3)*b(2)
    c(2)=a(3)*b(1)-a(1)*b(3)
    c(3)=a(1)*b(2)-a(2)*b(1)
    return
    end

```

12 Free Groups

A free abelian group is a direct sum of infinite cyclic groups. A free group on the set A is the set of finite words composed from "letters" of the alphabet A and inverses of these letters. Thus for $A = \{a_1, a_2, \dots\}$, a valid word is $a_3 a_{17}^{-1} a_{123}$. It is understood that aa^{-1} is the identity, which we write as 1. A reduced word is a word where adjacent pairs of the form aa^{-1} have been removed. See Rotman **The Theory of Groups** for a more rigorous discussion. Multiplication is word concatenation. A presentation of a group is a generator set A , and a set of relations. For example, consider the generating set $\{x, y\}$ and the relations $x^2 = 1$, $y^3 = 1$, and $x^{-1}y^{-1}xy = 1$ (that is, $xy = yx$). We shall show that this group is isomorphic to $\sigma(6)$, the cyclic group of order 6. First, every reduced word of length ≤ 3 is equivalent to one of

$$1, x, y, xy, y^2, xy^2.$$

The possibilities for words of length ≤ 3 , that differ from these, and do not contain substrings xx or yyy , are

$$xyx = xxy = y$$

$$yxy = xy^2 = xy^2$$

$$yx = xy$$

$$yyx = yxy = xyy.$$

Now consider words of length 4. They can be reduced to smaller words. Thus

$$xyxy = xxyy = y^2$$

$$xyyx = xxyy = y^2$$

$$yyxy = yyyx = x$$

$$yxyx = yxxy = y^2$$

So repeatedly reducing subgroups of length 4, we can reduce any word to a word of length 3 or less. Hence every reduced word is equal to one of the above six. Now we have

$$(xy)^2 = yy, (xy)^3 = yyxy = x, (xy)^4 = xxy = y, (xy)^5 = yxy = xyy, (xy)^6 = xyxy = 1$$

So this group is the cyclic group of order 6 generated by xy .

A free group can be defined in a more abstract way. A free group F on the set A is a set A and a function f from A to F , and having the following property. It is characterized by a commutative diagram. If $h : A \rightarrow G$ is any function, then there is a unique homomorphism r from F to G making the following diagram commute.

$$\begin{array}{ccc}
 & F & \\
 f \nearrow & & \searrow r \\
 A & \rightarrow & G \\
 & h &
 \end{array}$$

In the concrete realization of the free group generated by A , map r takes the word $s_1s_2\dots s_n$ to $h(a_1)h(a_2)\dots h(a_n)$, where $a_i \in A$ and $f(a_i) = s_i$. There is an obvious modification when s_i is an inverse symbol.

We can use the free group diagram to prove that all free groups on A are isomorphic by letting G be a second free group.

Every group is a quotient group of a free group. For let A be G , and let K be the kernel of r . Then F/K is isomorphic to G .

A group G is generated by A , and relations R , when it is a quotient group of a free group on A . Let F be free on A . Let R be a set of relations on G of the form $R = \{r_i = 1 : i \in I\}$. Let K be the normal subgroup generated by $\{r_i : i \in I\}$, then the generated group is $G = F/K$. (A, R) is called a presentation of G .

13 Actions and Orbits

Given a set M and a group G , the action of G on M is a mapping $\phi : G \times M \rightarrow M$ with the following properties.

$$\phi(a, \phi(b, m)) = \phi(ab, m)$$

and

$$\phi(e, m) = m.$$

We may abbreviate $\phi(a, m)$ as $am \in M$. For a fixed a , $\phi(a, \cdot)$ is a one to one mapping from M to M . This follows because from

$$am_1 = am_2$$

we have

$$m_1 = a^{-1}am_1 = a^{-1}am_2 = m_2.$$

Thus the mapping taking $g \in G$ to $\phi(g, \cdot)$ is a homomorphism from G into the set of 1 to 1 transformations of M . A group with an action is called a transformation group.

The orbit of an element $m \in M$ is the set of images am for all a in G . We write it as $G \cdot m$. The isotropy group G_m is the subgroup of G that preserves m , that is $g \in G_m$ iff $gm = m$. Let $\#S$ be the cardinality of set S . Then we have

Proposition For a finite group with an action we have for each $m \in M$

$$\#G = \#(G \cdot m)\#G_m.$$

A reference for these concepts is **Group Theory and Physics**.

14 The relation between the Lorentz group and $SL(2, C)$

See **Group Theory and Physics**, and **Relativity** by Emery.

15 Symmetry

The symmetry group (permutation group) of a set of points X , written as Σ_X , is the set of transformations from X to X that are 1 to 1 and onto. Thus given a set of integers $\{1, 2, 3, \dots, n\}$ its symmetry group is the permutation group S_n . A regular polygon with n vertices, including the sides of the polygon, has a symmetry group related to the permutation of the vertices. However, this symmetry group is normally not considered to be the set of all 1-1 onto maps of the polygon to itself. Symmetry groups of plane figures are groups of transformations that preserve shape. Hence they are isometries and thus linear mappings. They are subgroups of all orthogonal transformations. A symmetry group might also preserve more than just shape, for example it might be required to preserve the color of an image. Thus each point of a given color must map to another point of the same color.

16 Conjugates

17 Noether's Theorem

Certain symmetries imply conserved quantities. Two books, which I own, have interesting materials on Noether's theorem and contain a proof of it. One of them is **Analytical Mechanics** by Louis N Hand and Janet D Finch Cambridge, 1998. (Chapter 5 Noether's Theorem and Hamiltonian Dynamics.) The other is **Quantum Electrodynamics** by Sokolov and others.

18 Bibliography

- [1]Higman Bryan, **Applied Group Theoretic Methods**, 1964, Dover.
- [2]Cotton Albert, **Chemical Applications of Group Theory**, 1963, John

Wiley.

- [3] Lomont J S, **Applications of Finite Groups**, 1961, Dover.
- [4] Rotman Joseph J, **The Theory of Groups**, 2nd ed, 1963, Allyn and Bacon.
- [5] Scott W R, **Group Theory**, 1987, Dover.
- [6] Adler Irving, **Groups in the New Mathematics**, 1967, John Day.
- [7] Kaplansky Irving, **Infinite Abelian Groups**, revised edition, 1971, University of Michigan Press.
- [8] Griffith Phillip A, **Infinite Abelian Group Theory**, 1969, university of chicago press.
- [9] Burnside W, **Theory of Groups of Finite Order**, 2nd edition, 1911.
- [10] Ledermann Walter, **Introduction to the Theory of Finite Groups**, 2nd edition, 1953.
- [11] MacDonald Ian D, **The Theory of Groups**, 1988, Robert E Krieger Publishing.
- [12] Higgins Philip J, **Categories and Groupoids**, 1971, Van Nostrand Reinhold.
- [13] Rose John S, **A Course on Group Theory**, 1978 Chambridge, 1994 Dover.
- [14] Sternberg S, **Group Theory and Physics**, 1994, Cambridge.
- [15] Baumslag B, Chandler B, **Theory and Problems of Group Theory**, 1968, Schaum's McGraw-Hill.
- [16] Weyl Hermann, **The theory of groups and quantum Mechanics**, Dover, 1950.
- [17] Weyl Hermann, **Symmetry**, 1952, Princeton University press.
- [18] Weyl Hermann, **The Classical Groups**, 1946, Princeton University press.
- [19] Hofmann Karl heinrich, Mostert Paul S, **Elements of Compact Semigroups**, 1966, Charles Merril.
- [20] Polites George W, **An Inroduction to the Theory of Groups**, 1968, International textbook company.
- [21] Dixon John D, **Problems of Group Theory**, 1973, Dover.
- [22] Petrich Mario, **Introduction to Semigroups**, 1973, Bell and Howell.
- [23] Emery James D, **Relativity**, 2002.
- [24] Fuchs Laszlo, **Infinite Abelian Groups**, 1970, Volumes I and II, Academic Press.
- [25] Bechenbach Edwin (Editor), **Applied Combinatorial Mathematics**,

Wiley,1964.

[26]Tucker, Alan, **Applied Combinatorics**, 2nd edition, 1984, Wiley.

[27]Duffy, George H, **Applied Group Theory, For Physicists and Chemists**, 1992, Prentice-Hall, QC174.17 .S 9D83, Linda Hall.

[28]Aleksandrov A D, Kolmogorov A N, Laurent'ev M A Editors, translated by S H Gould et al. **Mathematics: Its Content, Methods, and Meaning**, 3 Volumes, Dorset Press, 1963,1990.