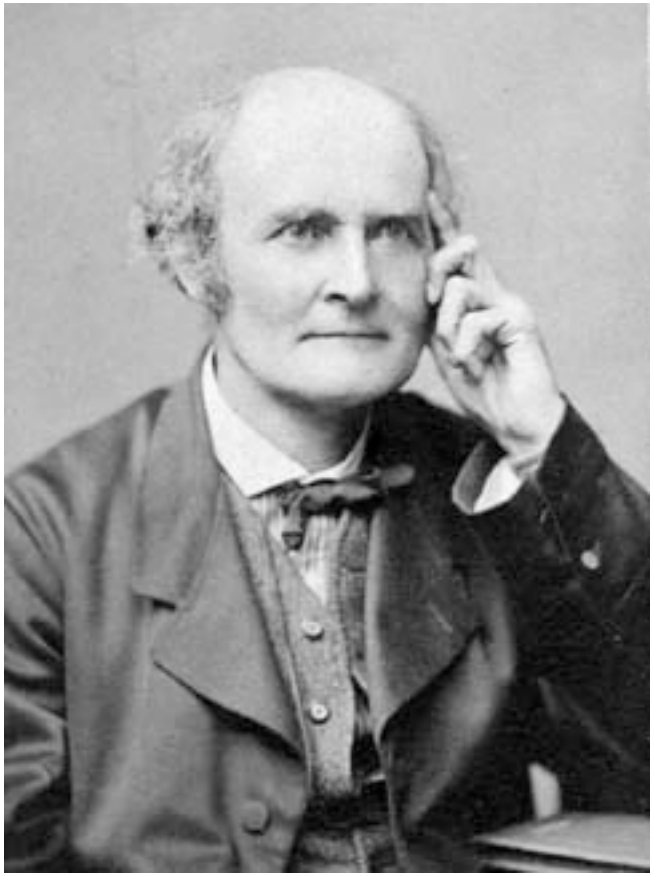
A group G is

- A set together with a binary map GxG G sending the pair (p,q) of elements of G into pq and satisfying:
- The associative law: (pq)r=p(qr)
- The existence of an identity element: there exists an element e in G such that ep=pe=p for all p in G
- The existence of a two sided inverse: for every p in G there is an element p^{-1} such that $p^{-1}p=pp^{-1}=e$.
- Group theory arose out of number theory, the theory of equations, crystallography, and geometry, but the first definition of an abstract group was given by Cayley in 1854.



Arthur Cayley 1821 - 1895

Examples: The special and general linear groups.

Let k be any field.
We will mainly be interested in

$$k = \mathbb{C},\ \mathbb{R},\ \mathbb{Q},\ \text{or}\ \mathbb{Z}/p\mathbb{Z}$$

where p is a prime. The group $Gl(n,k)$ is defined as the group of $n \times n$ invertible matrices with entries in k. The group $Sl(n,k)$ is the group of all $n \times n$ matrices with determinant equal to one. We write $Gl(n,p)$ or $Sl(n,p)$ instead of $Gl(n,\mathbb{Z}/p\mathbb{Z})$ or $Sl(n,\mathbb{Z}/p\mathbb{Z})$.

Examples: The unitary and orthogonal groups

The unitary group U(n) consists of all complex $n \times n$ matrices which satisfy

$$AA^{*}=I$$

where I is the identity matrix. The subgroup SU(n) consist of those elements of U(n) which have determinant one.

The orthogonal group O(n) consists of all real $n \times n$ matrices which satisfy

$$AA^{\dagger}= I.$$

The subgroup SO(n) consists of those elements of O(n) with determinant one. The columns of an element of O(n) are unit vectors and any two distinct columns are orthogonal. Similarly for U(n).

The group O(2).

If $A \in O(2)$ we can write the first column as

$$\begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$$

so there are two choices for the second column:

$$A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \quad \text{or} \quad A = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$$

The first case is rotation through angle θ.

The second case is reflection about the line through

$$\begin{pmatrix} \cos\theta/2 \\ \sin\theta/2 \end{pmatrix}.$$

The group SO(3)

A theorem of Euler asserts that if A $\in$ SO(3) and A $\neq$ I then A is rotation about some axis. To prove this, it is enough to show that there is a non-zero vector v such that Av=v, because then the line through v is fixed by A, as is the plane perpendicular to v, and the restriction of A to that plane acts as an element of SO(2) and so is a rotation. To show that v exists we must show that A-I has a non-zero kernel, i.e. that det(A-I)=0. But det A=det $A^{\dagger}$=1 so

$$\det(A-I) = \det(A^{\dagger}-I) = (\det A)(\det(A^{\dagger}-I) = \det[A(A^{\dagger}-I)] =$$

$$\det[AA^{\dagger}-A] = \det(I-A) = \det[(-I)(A-I) = \det(-I)\det(A-I) = -\det(A-I).$$

So det(A-I)=0 proving Euler's theorem.

The permutation groups

Let X be a set. S_X denotes the set of all 1 to 1 maps of X onto itself. Then S_X is a group where multiplication is composition: If $f, g \in S_X$ then

$$fg := f \circ g : \qquad x \mapsto f(g(x)).$$

If X is infinite, this group is huge, and so only of "theoretical" interest. But if X is finite, this is a very important object of study. Clearly if X and Y are in one to one correspondence the the groups S_X and S_X are the "same up to re-labeling".

If X is the n-element set $\{1, \ldots, n\}$ then S_X is denoted by S_n. It has $n!$ elements.

The ax+b group.

This is the group of all two by two matrices of the form

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \qquad a \neq 0$$

over any field. The product of two such matrices is again of the same type:

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} aa' & ab' + b \\ 0 & 1 \end{pmatrix}$$

so the inverse is given by

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a^{-1} & -a^{-1}b \\ 0 & 1 \end{pmatrix}.$$

The ax+b group, continued.

The name derives from the action of such a matrix on a vector with one in the second position:

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} ax+b \\ 1 \end{pmatrix}.$$

Over the reals this gives a "rescaling"

and change of origin.

The Affine group A(n).

We can generalize the $ax + b$ group by replacing 2 by $n + 1$, the scalar a by an invertible $n \times n$ matrix A and the scalar b by the column n-vector v.
Thus an element of Aff$(n)$is an $(n + 1) \times (n + 1)$ matrix of block form $\begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix}$,

the product of two such elements is given by

$$\begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A' & v' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} AA' & v + Av' \\ 0 & 1 \end{pmatrix},$$

and the inverse is given by

$$\begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} A^{-1} & -A^{-1}v \\ 0 & 1 \end{pmatrix}.$$

Aff(n), continued.

Also we have the action of an element of $\mathrm{Aff}(n)$ on a column n-vector x given by

$$\begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} Ax + v \\ 1 \end{pmatrix}.$$

So $x \mapsto Ax + v$, the result of applying the linear transformation A followed by translation through the vector v. To save space, we won't write the bottom row (0 1). We will write an element of $\mathrm{Aff}(n)$ as (A, v) with multiplication law

$$(A, v)(A', v') = (AA', v + Av').$$

The Euclidean group E(n).

This is the subgroup of Aff(n) where the A is restricted to be orthogonal. So an element of E(n) is of the form (A,v) where $AA^{\dagger}=I$. The action of (A,v) on a vector x is given by

$$(A,v)x = Ax+v.$$

First apply the linear transformation A to x and then apply the translation through the vector v. In group language,

$$(A,v)=(I,v)(A,0)$$

The group E(2) is the group of "congruences" of Euclidean plane geometry.

Let T denote the subgroup consisting of all translations, so T denotes the set of all elements of the form (I,v). Let H denote The subgroup consisting of all (A,0).

Conjugation and normal subgroups

Let G be any group. If $a \in G$, the conjugation action by a is the map of
G into itself given by

$$b \mapsto aba^{-1} .$$

We have

$$a(bc)a^{-1} = (aba^{-1})(aca^{-1}),$$

by the associative law. So conjugation by a is an **automorphism** of G.
A subgroup N of G is called **normal** if every element of N is carried into N by conjugation by every element of G. In symbols

$$n \in N \text{ implies } ana^{-1} \in N \quad \text{for all } a \in G.$$

We claim that T is a normal subgroup of Aff(n) and of E(n). Indeed,

$(A,w)(I,v)(A,w)^{-1} =$

$(A,w)(I,v)(A^{-1},-A^{-1}w) =(A,Av+w)(A^{-1},-A^{-1}w)= =(I, Av) \in N$.

The conjugation action action of an element (A,w) on $(I,v) \in T$ sends (I,v) into (I,Av).

Semi-direct product

We generalize the example of Aff(n) or E(n) as follows: Let N be a group. For applications we will assume that N is commutative, and write the group composition law as addition (i.e. with a "+" sign). Let H be some other group (not necessarily commutative) and write its group law as usual. Suppose that H "acts as automorphisms" of N. This means that any $A \in H$ sends $n \in N$ into an element An, and we have

$A(n+m)= An+Am$ and $A(Bn)=(AB)n$ for all $A,B \in H$ and $m,n \in N$.

Then we can construct a group whose elements are all pairs (A,n) with $A \in H$ and $n \in N$, and the multiplication law is

$$(A,m)(B,n) = (AB, An+m).$$

This group is called the **semi-direct product** of H and N. We can Identify N as the normal subgroup of this semi-direct product consisting of all elements of the form (I,n) where I is the identity element of H. Also H can be identified with the set of all elements of the form (A,0). Notice that in this identification $H \cap N$ consists only of the identity (I,0).

Semi-direct products from an internal viewpoint.

Conversely, suppose we start with a group G which contains a normal subgroup N, and also contains a subgroup H with the properties

$$H \cap N = \text{identity element, and } G = NH.$$

The second equation means that every element of G can be written as a product mA with $m \in N$ and $A \in H$. Then

$$mAnB = m(AnA^{-1})AB.$$

So if we define the action of H on N by $A \bullet n := AnA^{-1}$ (the notation is a little confusing) we see that G is the semi-direct product of H and N.

Example: $G = S_3$, $N = C_3$ the cyclic group of order three (consisting) of those permutations preserving the cyclic order, and $H = S_{\{2,3\}}$ the permutation group on the two elements 2 and 3.