Example 4.9. Let

$$1= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad I= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad J= \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \quad K= \begin{pmatrix} i & 0 \\ 0 & -I \end{pmatrix}$$

Then the relations $I^2=J^2=K^2=-1$, IJ=K, JK=I, KI=J, JI=-K, KJ=-I and IK=-J hold (verify). The set Q_8 = {±1, ±I , ±J, ±K } is a group called **Quaternion Group**. It is to be noted that Q_8 is a non-commutative group.

Example 4.10. Let C^* be the set of nonzero complex numbers. Under the operation of multiplication C^* forms a group. The identity is 1. If z = a + ib is a nonzero complex number, then

$$z^{-1} = \frac{a-ib}{a^2+b^2}$$

is the inverse of z. It is easy to see that the remaining group axioms hold.

A(S) (THE SET OF 1-1 MAPPINGS OF S ONTO ITSELF)

We focus our attention in this section on particularly nice mappings of a non empty set, S, into itself. Namely, we shall consider the set, *A(S),* of all 1-1 mappings of S onto itself. Although most of the concern in this note will be in the case in which S is a finite set, we do not restrict ourselves to that situation here.

When S has a finite number of elements, say *n,* then A(S) has a special name. It is called the ***symmetric group of degree n*** and is often denoted by S_n. Its elements are called ***permutations*** of S. If we are interested in the structure of S_n, it really does not matter much what our underlying set S is. So, you can think of S as being the set {1, ... , n}. In the investigation of finite groups, S_n plays a central role.

There are many properties of the set A(S) on which we could concentrate. We have chosen to develop those aspects here which will motivate the notion of a group and which will give the reader some experience, and feeling for, working in a group-theoretic framework.

Lemma 4.1. A(S) satisfies the following:

(a) f, g ϵ A(S) implies that fg ϵ A(S).

(b) f, g, h ϵ A(S) implies that(fg)h= f(gh).

(c) There exists an element, the identity mapping i, such that fi = if = f, for every f ϵ A (S).

(d) Given f ϵ A(S), there exists a g ϵ A(S) (g = f^{-1}) such that fg = gf= i.

Proof: Left as an exercise.

We should now like to know how many elements there are in A(S) when S is a finite set having *n* elements. To do so, we first make a slight digression.

Suppose that you can do a certain thing in *r* different ways and a second independent thing in *s* different ways. In how many distinct ways can you do both things together? The best way of finding out is to picture this in a concrete context. Suppose that there are *r* highways running from Kolkata to Mumbai and *s* highways running from Mumbai to Delhi. In how many ways can you go first to Mumbai, then to Delhi? Clearly, for every road you take from Kolkata to Mumbai you have *s* ways of continuing on to Delhi. You can start your trip from Kolkata in *r* distinct ways, hence you can complete it in *rs* different ways.

It is fairly clear that we can extend this from doing two independent things to doing *m* independent ones, for an integer $m > 2$. If we can do the first things in r_1 distinct ways, the second in r_2 ways, , the *m*-th in r_m distinct ways, then we can do all these together in $r_1\, r_2 \ldots\ldots. r_m$ different ways.

Lemma 4.2. If S has *n* elements, then *A(S)* has *n*! elements.

Proof: Let $f \in A(S)$, where $S = \{x_1, x_2, \ldots , x_n \}$. How many choices does *f* have as a place to send x_1? Clearly n, for we can send x_1 under *f* to any element of S. But now *f* is *not* free to send x_2 anywhere, for since *f* is 1-1, we must have $f(x_1) \neq f(x_2)$. So we can send x_2 anywhere except onto $f(x_1)$. Hence, *f* can send x_2 into $n-1$ different images. Continuing this way, we see that *f* can send x_i into $n - (i - 1)$ different images. Hence the number of such *f*'s is $n(n- 1)(n- 2)\ldots..1= n!$. □

Example 4.11. The number *n*! gets very large quickly. To be able to see the picture in its entirety, we look at the special case *n* = 3, where *n*! is still quite small.

Consider $A(S) = S_3$, where *S* consists of the three elements x_1, x_2, x_3. We list all the elements of S_3, writing out each mapping explicitly by what it does to each of x_1, x_2, x_3.

1. $i: x_1 \rightarrow x_1,\ x_2 \rightarrow x_2,\ x_3 \rightarrow x_3$
2. $f: x_1 \rightarrow x_2,\ x_2 \rightarrow x_3,\ x_3 \rightarrow x_1$
3. $g: x_1 \rightarrow x_2,\ x_2 \rightarrow x_1,\ x_3 \rightarrow x_3$
4. $gf: x_1 \rightarrow x_1,\ x_2 \rightarrow x_3,\ x_3 \rightarrow x_2$
5. $fg: x_1 \rightarrow x_3,\ x_2 \rightarrow x_2,\ x_3 \rightarrow x_1$
6. $ff/f^2: x_1 \rightarrow x_3,\ x_2 \rightarrow x_1,\ x_3 \rightarrow x_2$

Since we have listed here six different elements of S_3, and S_3 has only six elements, we have a complete list of all the elements of S_3. What does this list tell us?

To begin with, we note that *fg* ≠gf*,* so one familiar rule of the kind of arithmetic we have been used to is violated. Since g϶S_3 and g϶S_3, we must have *gg* (g^2) also in S_3. What is it? If we calculate *gg,* we easily get *gg* = *i.* Similarly, we get

$(fg)(fg) = i = (gf)(gf)$

Note also that $f\,(ff) = i$, hence $f^{-1} = ff$. Finally, we leave it to the reader to show that gf = $f^{-1}g$.

From now on we shall start using the shorthand of exponents, to avoid expressions like *ffffffff.* We define, for $f \in A\,(S)$, $f^0 = i$, $f^2 = ff$, and so on. For negative exponents $-n$ we define f^{-n} by $f^{-n} = (f^{-1})^n$, where n is a positive integer. The usual rules of exponents prevail, namely $f^r f^s = f^{r+s}$ and $(f^r)^s = f^{rs}$. We leave these as exercises-somewhat tedious ones at that-for the reader.

Caution! Do not jump to conclusions that all familiar properties of exponents go over.For instance, in the example of the *f,* g ϵ S_3 defined above, it can be easily verified that $(fg)^2 \neq f^2g^2$.

However, some other familiar properties do go over. For instance, if *f,* g, *h* are in *A(S)* and *fg = fh,* then g = *h.* Why? Because, from *fg = fh* we have $f^{-1}(fg) = f^{-1}(fh)$; therefore, g = $ig = (f^{-1}f)g = f^{-1}(fg) = f^{-1}(fh) = (f^{-1}f)h = ih = h$. Similarly, *gf = hf* implies that g = *h.* So we can cancel an element in such an equation provided that we *do not change sides.* In S_3 our *f,* g satisfy $gf = f^{-1}g$, but since $f \neq f^{-1}$ we *cannot cancel* the g here.