

## Groups

### a presentation to the MEI Conference 2007

by Peter Mitchell

pm@meikleriggs.co.uk

http://meikleriggs.co.uk

\*\*\*

Consider the transformations of the plane represented by reflection on the standard Cartesian axes. These gives two possibilities, viz

$$X : (x, y) \rightarrow (x, -y)$$

$$Y : (x, y) \rightarrow (-x, y)$$

Let us now consider what happens if they are applied in succession, ie we compose them in all possible pairs. We get

$$YX : (x, y) \rightarrow (x, -y) \rightarrow (-x, -y)$$

$$XY : (x, y) \rightarrow (-x, y) \rightarrow (-x, -y)$$

$$XX : (x, y) \rightarrow (-x, y) \rightarrow (-x, y)$$

$$YY : (x, y) \rightarrow (x, -y) \rightarrow (-x, y)$$

From this we see that the operation  $X$  is self-inverse, and so is  $Y$ . In addition,  $YX = XY$ , and we shall call that  $Z$ . If we define also the element  $I$  we have

$$I : (x, y) \rightarrow (x, y)$$

$$Z : (x, y) \rightarrow (-x, -y)$$

We call  $I$  the identity transformation and  $Z$  corresponds to a half-turn about the origin. If we explore all possible compositions of those four we get the following table of results. The first element to be applied is the one on the top row; the second in the first column.

	$I$	$X$	$Y$	$Z$
$I$	$I$	$X$	$Y$	$Z$
$X$	$X$	$I$	$Z$	$Y$
$Y$	$Y$	$Z$	$I$	$X$
$Z$	$Z$	$Y$	$X$	$I$

Two things are quite striking about the resulting table. Each element appears exactly once in each row and each column – the *latin square property* – and the system is closed in so far as any combination of two elements of the four results in a further element of the four.

Other examples of the same kind of *generalised multiplication* can be constructed. Here are two more.

Consider the set of elements of the set  $P = \{1, 2, 3, 4\}$  and arithmetic modulo 5. That is defined as follows. If  $x, y \in P$  then  $xy = xy \bmod 5$  (which is the remainder when  $xy$  is divided by 5 – so  $3 \times 2 = 1$  because 6 divided by 5 gives remainder 1). The result is another closed system with the table below.

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

The same properties are evident here; moreover while the two tables are based each on four elements it is clear that they are just not the “same”.

Consider now the following six functions and their composition in pairs.

$$i: x \rightarrow x$$

$$f: x \rightarrow 1-x$$

$$g: x \rightarrow \frac{1}{x}$$

$$h: x \rightarrow \frac{1}{1-x}$$

$$j: x \rightarrow 1-\frac{1}{x}$$

$$k: x \rightarrow \frac{x}{x-1}$$

	<i>i</i>	<i>f</i>	<i>g</i>	<i>h</i>	<i>j</i>	<i>k</i>
<i>i</i>	<i>i</i>	<i>f</i>	<i>g</i>	<i>h</i>	<i>j</i>	<i>k</i>
<i>f</i>	<i>f</i>	<i>i</i>	<i>j</i>	<i>k</i>	<i>g</i>	<i>h</i>
<i>g</i>	<i>g</i>	<i>h</i>	<i>i</i>	<i>f</i>	<i>k</i>	<i>j</i>
<i>h</i>	<i>h</i>	<i>g</i>	<i>k</i>	<i>j</i>	<i>i</i>	<i>f</i>
<i>j</i>	<i>j</i>	<i>k</i>	<i>f</i>	<i>i</i>	<i>h</i>	<i>g</i>
<i>k</i>	<i>k</i>	<i>j</i>	<i>h</i>	<i>g</i>	<i>f</i>	<i>i</i>

This table has the same properties as those listed above. Each of those *Cayley tables* is an example of a *group*. The rule for combination is a *binary operation* on the set denoted by *G*, say, which has the following properties. (The dot corresponds to “such that”).

1. The system is closed, ie  $x, y \in G \Rightarrow xy \in G$ ;
2. there is an identity element, ie  $\exists e \in G \cdot xe = ex = x \forall x \in G$ ;
3. each element has an inverse, ie  $x \in G \Rightarrow \exists x^{-1} \in G \cdot xx^{-1} = x^{-1}x = e$ ;
4. the operation is associative, ie  $x, y, z \in G \Rightarrow (xy)z = x(yz)$

That set of properties characterises a group for a set *G* with a binary operation defined on it. If the group is finite – it need not be – the number of elements is termed its *order*.

Note that commutativity is *not* required. Indeed, for the group of six functions with the operation of composition, for example,  $gh \neq hg$ . A group in which the binary operation *is* commutative is called an *abelian* or *commutative* group. Both the first two examples of order four were in fact abelian.

Why is the associative law required? Consider the example of the set  $\{0,1,2,3,4\}$  with the binary operation  $a.b = |a - b|$ . Here is the table.

	0	1	2	3	4
0	0	1	2	3	4
1	1	0	1	2	3
2	2	1	0	1	2
3	3	2	1	0	1
4	4	3	2	1	0

This shows many of the properties of a group. The operation is certainly closed, 0 is the identity element, and each element is self-inverse. It does not have the latin square property (that each row and each column is a permutation of the elements of the group) which we have seen in every example so far. Rather less obviously It does not satisfy the associative law, since, for example,  $|3 - |1 - 1|| = 3 \quad ||3 - 1| - 1| = 1$ . So this pairing of set and

operation does *not* give a group.

The last two observations are closely connected. We shall show that the associative law is essential to establish the latin square property.

Suppose that there are indeed two identical elements in some row. We can argue that this is not possible by equating the elements in the  $a$  and  $b$  columns of the table, to show that  $a$  and  $b$  are then identical.

$$\begin{aligned} xa &= xb \\ \Rightarrow x^{-1}(xa) &= x^{-1}(xb) \\ \Rightarrow (x^{-1}x)a &= (x^{-1}x)b \\ \Rightarrow a &= b \end{aligned}$$

Here are some further examples of group properties derived by logical argument from the defining properties.

*In a group  $G$  the identity element is unique.*

Suppose that there are two elements with the identity property. We show that they are identical. Assume that

$$\exists e_1, e_2 \in G \cdot e_1 x = x = x e_1, e_2 x = x = x e_2 \quad \forall x \in G.$$

Then

$$e_1 \in G \Rightarrow e_1 e_2 = e_2 e_1 = e_1$$

(by the defining property of  $e_2$ ) and

$$e_2 \in G \Rightarrow e_1 e_2 = e_2 e_1 = e_2$$

(by the defining property of  $e_1$ ) ie

$$e_1 = e_1 e_2 = e_2 e_1 = e_2$$

so the elements  $e_1, e_2$  are identical.

A similar argument shows that *the inverse for one particular element must be unique.*

Suppose that given  $x \in G \exists y, z \cdot xy = yx = e$  and  $xz = zx = e$ .

Then we have

$$y = ye = yxz = ez = z$$

So the two elements are not distinct after all.

It was earlier remarked that the two groups of order four considered were clearly different. Now consider another group based on modulo arithmetic, this time mod 7. Here is its Cayley table, accompanied by the earlier six element function group.

	1	2	3	4	5	6		$i$	$f$	$g$	$h$	$j$	$k$
1	1	2	3	4	5	6	$i$	$i$	$f$	$g$	$h$	$j$	$k$
2	2	4	6	1	3	5	$f$	$f$	$i$	$j$	$k$	$g$	$h$
3	3	6	2	5	1	4	$g$	$g$	$h$	$i$	$f$	$k$	$j$
4	4	1	5	2	6	3	$h$	$h$	$g$	$k$	$j$	$i$	$f$
5	5	3	1	6	4	2	$j$	$j$	$k$	$f$	$i$	$h$	$g$
6	6	5	4	3	2	1	$k$	$k$	$j$	$h$	$g$	$f$	$i$

In this case we can again observe that the two structures are different. That claim is justified by observing that in the function group three elements are self-inverse but in arithmetic mod 7 only two are.

Now consider the structure more closely in each case.

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

	i	f	g	h	j	k
i	i	f	g	h	j	k
f	f	i	j	k	g	h
g	g	h	i	f	k	j
h	h	g	k	j	i	f
j	j	k	f	i	h	g
k	k	j	h	g	f	i

If we confine attention to the subsets which are shaded, they demonstrate closure in each case. They are examples of *subgroups*, subsets of the original group which are themselves self-sufficient as groups.

They also show a further property. Consider the two subgroups in comparison.

	1	2	4
1	1	2	4
2	2	4	1
4	4	1	2

	i	h	j
i	i	h	j
h	h	j	i
j	j	i	h

These two groups are essentially the same, by inspection, but we must specify what we mean by that. If we consider the mapping defined by

$$\phi : 1 \leftrightarrow i, 2 \leftrightarrow h, 4 \leftrightarrow j$$

then for every possible pairing  $a, b$  we have

$$\phi(ab) = \phi(a)\phi(b).$$

What we mean by "same" is expressed here as essentially the preserving of structure. The binary operation is what converts a set into a group: the binary operation in this pairing works with exactly the same structure in each, because products of elements in one correspond to products of the corresponding elements in the other.

Such a structure preserving map is a *homomorphism* (which may be a many-one map) and in this case also an *isomorphism* (because it is also one-one).

Some basic properties of homomorphisms (and consequently for isomorphisms) are easily established from definitions and logical argument as before.

For example, if  $a \in G$  and  $e$  is the identity element, for a homomorphism  $\phi$  of  $G$

$$\text{onto } K, \phi(a) = \phi(ae) = \phi(a)\phi(e), \quad \phi(a) = \phi(ea) = \phi(e)\phi(a)$$

so now we can see that  $\phi(e)$  is the identity element in the image  $K$  (because it behaves like the identity element and the identity element is unique).

Again, if  $a \in G$ ,  $e$  is the identity element, and  $a^{-1}$  the inverse

$$\phi(e) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1}), \quad \phi(e) = \phi(a^{-1}a) = \phi(a^{-1})\phi(a)$$

so  $\phi(a^{-1})$  has the defining property of  $\phi(a)^{-1}$  so by the uniqueness of an inverse that is indeed what it is. Hence a homomorphism maps inverses onto inverses.

We can see too from this simple example that such a pair of isomorphic groups may be isomorphic in more than one way. Compare the two in slightly revised form:

	1	4	2
1	1	4	2
4	4	2	1
2	2	1	4

	<i>i</i>	<i>h</i>	<i>j</i>
<i>i</i>	<i>i</i>	<i>h</i>	<i>j</i>
<i>h</i>	<i>h</i>	<i>j</i>	<i>i</i>
<i>j</i>	<i>j</i>	<i>i</i>	<i>h</i>

Now it is also clear that the mapping  $\psi : 1 \leftrightarrow i, 2 \leftrightarrow j, 4 \leftrightarrow h$  is a second one-one structure-preserving map, ie an isomorphism.

Consider again arithmetic modulo 7.

	1	2	3	4	5	6	Notice that
1	1	2	3	4	5	6	$3^2 = 2,$
2	2	4	6	1	3	5	$3^3 = 3 \times 2 = 6,$
3	3	6	2	5	1	4	$3^4 = 3 \times 6 = 4,$
4	4	1	5	2	6	3	$3^5 = 3 \times 4 = 5,$
5	5	3	1	6	4	2	$3^6 = 3 \times 5 = 1.$
6	6	5	4	3	2	1	

This illustrates a *cyclic* group, one which is generated entirely by powers of one single (non-identity) element. It is also generated similarly by the element 5. And there is one subgroup of order generated by either 2 or 4. By contrast the transformation group considered first is a non-cyclic group (as can be verified by trying to generate it by using powers of each of the non-identity elements) of order four.

Related to this is the idea of the *order* of an element in a group – in a finite group generating powers of an element in this way must lead eventually to the identity element. The order of an element is the least power needed to do that. In the transformation group each of the three non-identity elements has order two.

\*\*\*

This short introduction to the ideas of groups shows that almost all the properties can be introduced to students by way of examples and without stating them explicitly other than in response to student observation.

This approach paves the way for the introduction of *Lagrange's Theorem* – that the order of a subgroup of a finite group must divide the order of the group – as the only major result at this level.