1. INTRODUCTION TO GROUPS

§1.1. Group Theory: The Door to Abstract Mathematics

So you've decided to study group theory! Whether or not you made a free choice, or whether it just happens to be part of a course you have to study, is immaterial. The important thing is that you're properly introduced to the subject and that you develop an overview into which you can retreat whenever you get lost in the details.

I could begin this introduction by telling you what a group is. In fact I will. Whether you'll be any the wiser remains to be seen!

A GROUP (G, ∗) is a set G together with a binary operation ∗ which is associative, has an identity and has inverses for all its elements.

There now. You know what a group is. All of group theory is built on that one brief statement. Yet it's likely that you don't feel very comfortable about groups at this stage. Numbers have been your friends for as long as you've known any mathematics and, more recently, you've learnt to deal with mathematical objects like functions, matrices and vectors. But groups are sets whose elements aren't specified. Are they numbers? Possibly. Are they matrices? They might be. It all sounds a bit vague and abstract.

Of course once you've been given some examples you'll feel a little happier. But before we do that it would be helpful if we talked about the nature of abstraction. One thing you'll soon discover is that groups are essentially *abstract* entities.

The word 'abstract' usually conveys the idea of something that's abstruse, vague and very difficult. In fact it's more accurate to associate 'abstract' with words such as 'powerful', 'virtual', and even 'beautiful'.

The ability to handle abstraction is possibly the greatest thing that sets humans apart from other creatures. Language is a system whereby concrete experiences are abstracted and are represented by sounds or squiggles. Numbers may seem to be very concrete but a moment's reflection will show you how sophisticated and abstract they are. Once we move beyond 'two apples' or 'two monkeys' to just 'two' we've come a long way in the process of abstraction. And all that before the age of five!

All areas of knowledge involve ever deeper levels of abstraction. Our modern world is becoming increasingly abstract. Money can be electronic. Reality can be virtual. Atomic particles are now considered to behave more like waves than little billiard balls.

What is the real ‘stuff’ of mathematics – the fundamental objects of study? For most of your mathematical life you would have said ‘numbers’. Of course ‘number’ has meant different things to you at different times – from ‘things you count with’, to ‘positions on the number line’ and finally to ‘elements of the field of complex numbers’. But all this time you lived within this system of complex numbers and you explored every far corner.

The system of complex numbers is by far the most important mathematical system of all, but it’s still only *one* system. More recently you’ve encountered other systems – systems of matrices, systems of polynomials and so on. In abstract algebra we don’t just study further *examples* of algebraic systems but rather we study algebraic *systems* themselves.

In group theory we restrict our attention to systems with just one binary operation satisfying certain key properties. A binary operation $*$ on a set S is a function from $S \times S$ to S, or more informally, it’s an operation that combines any (ordered) pair of elements $a, b \in S$ to produce an element $a * b \in S$.

Other branches of abstract algebra, such as ring theory, consider systems with two or more operations but in group theory we see how far we can get with just one. After all, if we have a system with two binary operations, we can always close one eye and focus on one operation at a time.

But why do we insist that they possess certain properties? Surely if we make no conditions our theory would be more general. That's true, but the trouble is that too much generality can lead to shallowness. A rich theory depends on having just the right amount. And, as the mathematicians who shaped group theory discovered, there are four properties which lead to a theory which, on the one hand is very rich and beautiful, and on the other, is very useful and applicable.

These four properties are called the 'group axioms'. But don't think of these axioms as somehow self-evident truths in the way that many people think of the axioms of geometry. They're simply four properties that a system with a single binary operation must possess before it's allowed to be called a 'group'.

There was a time when groups were more concrete. When Évariste Galois invented the concept of a group, in the early 1800s, groups consisted of permutations (or 'substitutions') of the zeros of a polynomial. Then it was realized that most of the theory doesn't need to assume anything about the nature of the things being permuted. Here was the first level of abstraction. Groups became sets of permutations of 'things'.

Then, towards the end of the nineteenth century, group theorists began to realise that a considerable portion of that theory, by now well developed, could be built up from just four basic facts about permutations. So the theory will apply to any other algebraic system that satisfies those properties. No longer do the elements have to be permutations, although an important branch of group theory has to do with permutation groups.

What are these four axioms? The first, closure, is really implicit in the concept of a binary operation. You'll notice that we didn't explicitly refer to it in our brief definition above. It simply insists that the result of combining two elements of a group should again be in the group.

CLOSURE: $a * b \in \mathrm{G}$ for all $a, b \in \mathrm{G}$.

Here we're using $*$ to refer to the binary operation and, of course, $\in$ denotes set membership. Without closure we wouldn't be able to consider an expression like $(a * b) * c$ because if $a * b$ lies outside of G the result of combining it with c wouldn't be defined.

If the operation had been ordinary addition or multiplication of numbers we'd normally remove the parentheses here. The expression $a + b + c$ is unambiguous because both ways of interpreting it have the same value. That is, $(a + b) + c = a + (b + c)$. Addition and multiplication of numbers and polynomials and matrices are associative – but not every useful operation in mathematics is. For example $(a - b) - c$ is not the same as $a - (b - c)$ and so subtraction isn't associative. The vector product $\boldsymbol{u} \times \boldsymbol{v}$ for $\mathbb{R}^3$ is also a useful operation that fails to be associative.

Nevertheless we'll insist on the associative law before a system can be awarded the title 'group'. One fortunate result of this is that it allows us to have unambiguous powers. We'll denote an expression $a * a * a * \ldots * a$, with n factors, as a^n by analogy with multiplication of numbers. Without the associative law this would be highly ambiguous.

For example does a^4 mean $((a * a) * a) * a$ or perhaps $(a * a) * (a * a)$ or maybe it could be $(a * (a * a)) * a$ or could it mean $a * ((a * a) * a)$ or even $a * (a * (a * a))$? Without the associative law these might represent 5 different elements!

ASSOCIATIVITY:
$(a * b) * c = a * (b * c)$ for all $a, b, c \in$ G.

In ordinary algebra we're usually able to reverse the fundamental operations. Addition can be reversed by subtraction and multiplication by a non-zero number can be reversed by division. We can do these things because of inverses such as $-x$ and $1/x$. Inverses are vital to group theory and so we build them into the axioms. But before we can even talk about inverses we must have an identity element.

IDENTITY: There exists $e \in \mathrm{G}$ such that:

$$e * a = a = a * e \text{ for all } a \in \mathrm{G}.$$

You're used to writing the identity as 0 or 1 but for the moment we will use the neutral symbol *e* for the identity to avoid confusion. This is because you can have groups of numbers with some strange binary operation, neither addition nor multiplication, where the identity is neither 0 nor 1.

INVERSES: For all $a \in \mathrm{G}$ there exists $b \in \mathrm{G}$ such that

$$a * b = e = b * a.$$

With groups of numbers under addition (this just means we're focussing on addition as our operation) the identity is 0. In other groups it's the zero matrix or the zero vector. With groups of numbers under multiplication the identity is 1 and with matrix groups under matrix multiplication the identity is the identity matrix I.

With groups of numbers under addition the inverse of x is $-x$. Under multiplication it's x^{-1} or $1/x$.

But not every real number has an inverse under multiplication. The number zero doesn't have one. All this means is that when talking about the real numbers under multiplication we must exclude zero if we want to make a group. The system of *all* real numbers is a group under addition. The system of all *non-zero* real numbers is a group under multiplication.

Let's assemble all these axioms in one place to give a more explicit definition of a group.

A **group** (G, $*$) is a set G together with a binary operation $*$ such that the following hold:

CLOSURE LAW: $a * b \in$ G for all $a, b \in$ G.
ASSOCIATIVE LAW:
$(a * b) * c = a * (b * c)$ for all $a, b, c \in$ G.
IDENTITY LAW: There exists $e \in$ G such that
$e * a = a = a * e$ for all $a \in$ G.
INVERSE LAW: For all $a \in$ G there exists $b \in$ G such that $a * b = e = b * a$.

Notice that we don't assume the Commutative Law: $a * b = b * a$ for all a, b. An **abelian group** (named after the Norwegian mathematician Abel) is a group in which the following holds:

COMMUTATIVE LAW: $a * b = b * a$ for all $a, b \in$ G.

It's clear that you've been on close terms with groups most of your mathematical life. The first mathematical system you met was the system of counting numbers. Because you didn't know about negative numbers at that stage you would have to wait to meet your first group. Probably the first group you ever met was the group of positive rational numbers (fractions) where the operation is multiplication. The axioms were never mentioned in primary school, but you knew that when you multiplied two fractions you always got a fraction.

Because products such as $\frac{2}{3}\times\frac{1}{2}\times\frac{3}{4}$ were written without parentheses it probably never occurred to you that potentially you might have obtained a different answer if you'd multiplied $\frac{2}{3}$ by $\frac{1}{2}$ first rather than $\frac{1}{2}$ by $\frac{3}{4}$. The fact that you didn't, and that it produced $\frac{1}{4}$ however you did it, reinforced your instinctive acceptance of the associative law. And the 'invert and multiply rule' assured you that inverses always exist.

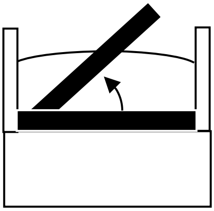
The next group that you encountered was probably the group of integers under addition as you learnt about negative numbers. Then, as you extended your mathematical horizons you encountered many other groups of numbers.

But groups needn't consist of numbers. There are groups of matrices and groups of functions. In fact, to emphasize the wonderfully abstract nature (i.e. generality) of the group concept, here's an example of a group where the elements appear to be as nonmathematical as you could imagine. They're different ways of turning a mattress!

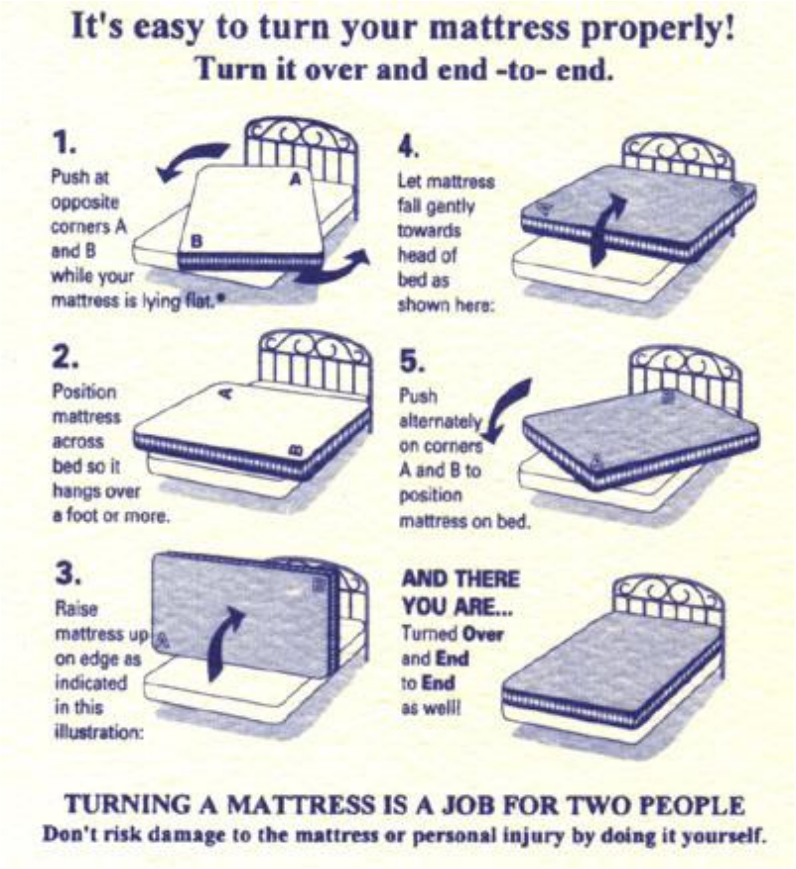
§1.2. The Dutch Wife's Mattress Problem

For centuries Dutch wives have been renowned for being very clean and very methodical and one of their basic household chores was turning over the mattresses every month to promote even wear. This problem concerns the best way to do it. These days households are too busy to be bothered doing this and this monthly ritual has largely disappeared along with the chores of ironing tea-towels or darning socks. But even if it is a problem that no longer has a practical significance it will help us to understand the concept of a group.

I should point out that although I have called it the Dutch *Wife's* Problem I don't mean to imply that doing housework is only woman's work. I got taken to task by one of my readers who resented this implication. The only reason why I call it "The Dutch Wife's Mattress Problem" is because my wife, now keeping Heaven clean and tidy, was Dutch and I used to have to help her with rotating the mattress.



The easiest rotation to perform is the one where you turn the mattress over, left to right when you stand at the foot of the bed.



It's easy to turn your mattress properly!
Turn it over and end -to- end.

1. Push at opposite corners A and B while your mattress is lying flat.*

2. Position mattress across bed so it hangs over a foot or more.

3. Raise mattress up on edge as indicated in this illustration:

4. Let mattress fall gently towards head of bed as shown here:

5. Push alternately on corners A and B to position mattress on bed.

AND THERE YOU ARE... Turned **Over** and **End** to **End** as well!

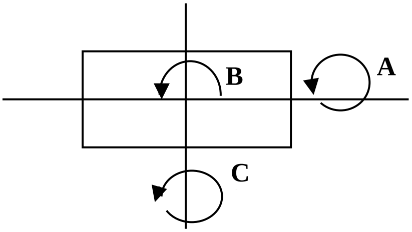
TURNING A MATTRESS IS A JOB FOR TWO PEOPLE
Don't risk damage to the mattress or personal injury by doing it yourself.

But if you did this every time, the head end would never change with the foot. So it’s necessary sometimes for the two of you to pick up the mattress and walk around the bed, rotating the mattress head to foot.

But a Dutch wife is very thorough. She knows that there’s a third rotation that can be performed. This involves lifting up the head end so that the mattress becomes vertical (perhaps narrowly missing the ceiling light) and then bringing it down so that it's now at the foot of the bed. The mattress is now upside down relative to the way it was, with head and foot reversed.

The Dutch Wife's Problem is to devise a mattress-turning regime so that the mattress wears uniformly. One could use all three rotations in turn but, as we'll see, this doesn't achieve even wear.

There are three basic mattress turns. The simplest, turning the mattress over, along its longer axis, we shall call A. Turning it head to foot, while keeping the mattress level, we shall call B. The one that nearly knocks out the light fitting, we'll call C.



The system mentioned above involves a three-monthly cycle such as:

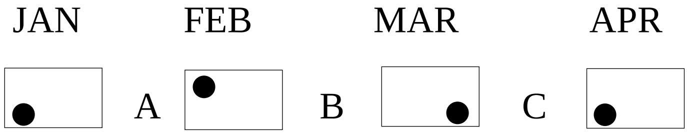
A, B, C, A, B, C, ...

Now there are two things wrong with such a plan.

(1) It's not necessary to do a C. You can achieve the same result as a C without risking the ceiling light, simply by doing A followed by B.

(2) More importantly it doesn't achieve what it sets out to do (ensuring that the mattress wears evenly) because at the end of each three-month period the mattress is back

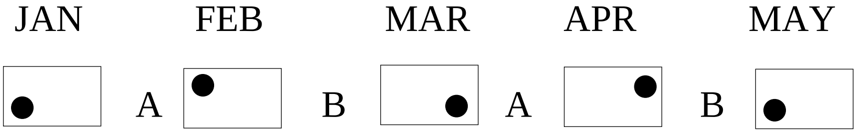
the way it was. Since there are four possible positions, one position gets missed out completely and it's the same one each time! One side of the mattress will get two months wear to every month on the other side. To see this clearly I've marked one corner of the mattress.



←   3 MONTH CYCLE   →

So what should all good mattress turners do? Simply leave out the most difficult rotation, C, and adopt the pattern: A, B, A, B, ...

Just because C is possible doesn't mean we should use it. But won't this mean that things will repeat after only two months? Not at all. The above regime will cause the mattress to go through all four positions once before repeating. We achieve our goal of even wear.



← EVEN WEAR OVER 4 MONTHS   →

The group here has four elements, each of which is a way of turning the mattress. “Four?” you say, “A, B, C – what’s the fourth?”. The fourth is I which is the identity operation that does nothing. It’s the operation that less conscientious people use – those who can’t be bothered turning the mattress at all. Although it sounds trivial the identity operation is as important to our little group as the number 1 is to arithmetic.

So our group contains four things, or as we shall say, we have a group of “order 4”. The elements of our little mattress group are I, A, B and C and the operation is to follow one rotation by another – finding a single rotation which would have achieved the same result. By experimenting with a real mattress, or better still with a paper model, or even better still by simulating a rectangle in our imagination, we conclude that A followed by B achieves the same result as C which we express as

$$A * B = C.$$

And A followed by A again reverts the mattress back to the way it was. Two A’s in succession is equivalent to doing nothing, that is

$$A * A = I$$

which we can express more simply as $A^2 = I$.

That's not to say that A followed by another A is equivalent *in all respects* to I. There's a lot less effort involved in doing I than in A^2. So we're losing some information here. But in terms of where things are at the end of it all, A^2 is the same as I.

Since there's no danger of confusion we can omit the $*$ and simply write these equations as $AB = C$ and $A^2 = I$. This notation makes it look very much like ordinary algebra, but we must be a little careful. The second equation tempts us to conclude that $A = \pm I$. But this is nonsense. There's no such thing as $-I$ in our mattress group. You mustn't expect the algebra of a group to always behave like ordinary algebra, the algebra of numbers. To some extent you'll have to learn algebra all over again in this new context.

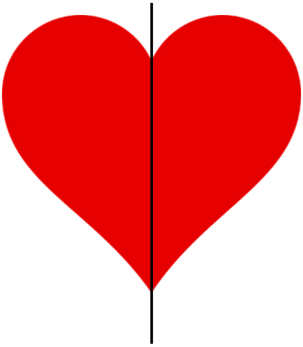
We can summarize our little algebraic system by means of a **group table**:

	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	C	I	A
C	C	B	A	I

If x represents one of the 'numbers' in our little group then the equation $x^2 = I$ has four solutions. But who ever heard of a quadratic equation having more than two solutions? Of course it can't happen in ordinary algebra. But we're now beginning to realise that the algebra we learnt at school doesn't apply universally. It applies to the system of real numbers and it applies to the system of complex numbers. In fact the core of high-school algebra (provided you leave out the inequalities) works for any system that satisfies the field axioms. But groups aren't fields and the algebra of groups can be a little more dangerous than the algebra of a field. Of course, danger spells excitement!

§1.3. The Dihedral Group of Order 8.

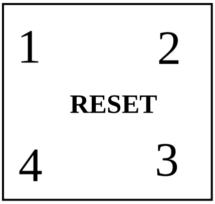
In the above discussion we assumed that the mattress was rectangular. A heart-shaped mattress would be more exotic but it would rule out rotating head to foot. The group in this case would contain only the 180° rotation about the axis of symmetry, and of course the identity.



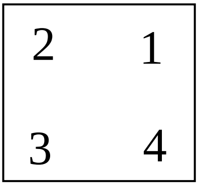
A circular mattress has a very high degree of symmetry and its group would be infinite! In principle we could rotate the mattress through any angle or turn it over around any one of the infinitely many axes of symmetry.

But let's go for a shape that has a little more symmetry than the rectangle, but not as much as the circle. Let's imagine a *square* mattress. In fact we can drop the references to beds and mattresses because what’s going on here is pure geometry.

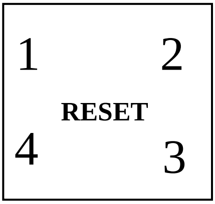
Let’s imagine a square, or better still, let’s cut out a little square from cardboard and label the corners 1, 2, 3, 4 in order. Also write the word RESET in the middle



Now turn the paper over and label the corners on the other side. You must ensure that this labelling is consistent with the first, so that corner 1 is corner 1 no matter which side of the paper you are looking at, and so on. Don’t write the word RESET on this side.

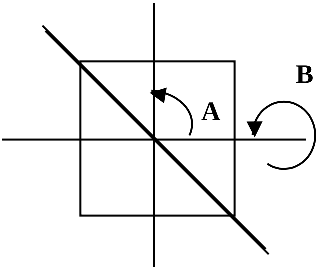


Now whenever I say RESET rotate your square, turning it over if necessary, so that you can read the word RESET the right way up. This is the reset position.



The rotation group of the square consists of all rotations which, at the end, leave the square occupying the same space as at the beginning (ignoring the labels).

A square has four axes of symmetry, vertical, horizontal and both diagonals. All four axes pass through the centre. If you flip the square about one of these axes the square will appear to be the same, although the labels will be different. These four 180° rotations belong to the rotation group. In addition there are rotations in the plane of the square, about the centre, through 90°, 180°, 270° and, not forgetting the identity, 0°. This gives us a group of order 8 (that is, 8 elements).



Let A denote the positive (anti-clockwise) 90° rotation about the centre. Then A^2 is the 180° rotation and A^3 is the 270° anti-clockwise rotation (or equivalently a clockwise 90° rotation). Let B denote the 180° rotation about the horizontal axis. One can easily verify that the 180° rotation about the vertical axis is A^2B and that AB and A^3B are the 180° rotations about the two diagonals.

The rotation group of the square is thus

$$\{I, A, A^2, A^3, B, AB, A^2B, A^3B\}$$

and its group table is:

	I	A	A^2	A^3	B	AB	A^2B	A^3B
I	I	A	A^2	A^3	B	AB	A^2B	A^3B
A	A	A^2	A^3	I	AB	A^2B	A^3B	B
A^2	A^2	A^3	I	A	A^2B	A^3B	B	AB
A^3	A^3	I	A	A^2	A^3B	B	AB	A^2B
B	B	A^3B	A^2B	AB	I	A^3	A^2	A
AB	AB	B	A^3B	A^2B	A	I	A^3	A^2
A^2B	A^2B	AB	B	A^3B	A^2	A	I	A^3
A^3B	A^3B	A^2B	AB	B	A^3	A^2	A	I

All of these can be verified using your little square. For example, reset the square to its initial position and perform operation AB, that is, A followed by B. Note down the positions of the 4 corners. Now reset the square again and perform operation A^3. This is A done 3 times. You should see that the positions of the corners are as before. So you will see that AB times A^3 is A^2B

Notice from the table that BA = A^3B. You can verify this using your square if you wish. But $A^3 = A^{-1}$ (a 270° rotation clockwise is the same as a 90° rotation anti-clockwise) so BA = $A^3B = A^{-1}B$.

Notice that this is different to AB, showing that AB $\neq$ BA. The commutative law breaks down in this group. This lack of commutativity is something that never occurs with numbers. But then there's no reason why rotations should behave like numbers. In general binary operations don't obey the commutative law. Numbers are the exception – rotations follow the general rule of not commuting.

Even in life things are usually non-commutative. It usually *does* matter in which order you do things. For example if

O = open the door and W = walk through the door

then OW (open the door and then walk through) is usually less painful than WO. And, especially in previous generations, many lives have been complicated by the lack of the commutative law when

M = get married and B = have a baby!

Once again we're reminded that we must learn algebra all over again. In many ways the algebra of groups is simpler than the algebra of numbers because we only have one operation. But in other ways it's more complicated. We're so used to using the commutative law for numbers that we wouldn't hesitate to cancel the x and x^{-1} in the expression $x^{-1}yx$ and, for numbers, that would be perfectly justified. On the other hand, in a non-commutative group this remote cancellation would not be justified and it could very well happen that $x^{-1}yx$ is quite different to y. Certainly we can cancel an x with its inverse, *but only if they are adjacent*.

Although there are eight elements in this group we've managed to express them all in terms of just A and B. We call these **generators** for the group. There are many relations that hold between these generators but all of them can be deduced from just these three:

$$A^4 = I, \quad B^2 = I, \quad BA = A^{-1}B$$

So we can summarise this group by writing it as

$$\langle A, B \mid A^4 = 1, B^2 = 1, BA = A^{-1}B\rangle.$$

We call this a **presentation** for G and read this as "the group generated by A and B such that $A^4 = 1$, etc". (When we write a presentation we usually use the symbol 1 for the identity.)

This presentation is a very compact way of describing the group because the entire group table can be deduced from it. Notice that the relation $BA = A^{-1}B$ can be regarded as the rule: moving a B past an A inverts the A. (But don't treat this as a universal rule of group theory. It just applies whenever we have $BA = A^{-1}B$.)

Using this rule, together with the other relations, we can verify every product in the group table without the need to rotate an actual square. For example:

$$\begin{aligned}(A^2B)(A^3B) &= A^2(BA^3)B \\ &= A^2(A^{-3}B)B \\ &= (A^2A^{-3})(BB) \\ &=A^{-1} = A^3.\end{aligned}$$

Where we represent a group in terms of generators and relations we call it a **presentation**. We list the generators to the left of the bar and the relations to the right. Sometimes the relations are equations. But if the right hand side of the equation is the identity we leave this out and call the left hand side a **relator**. So in a presentation we can use a mixture of relations and relators.

For the rotation group of the square we could write the presentation more simply as

$$\langle A, B \mid A^4, B^2, BA = A^{-1}B\rangle.$$

We could even change the equation $BA = A^{-1}B$ into the relator $B^{-1}ABA$ because $BA = A^{-1}B$ can be rewritten as $B^{-1}ABA = 1$. However it is more convenient to leave it as $BA = A^{-1}B$ because it provides a recipe for moving a B past an A.

This group is called the dihedral group of order 8. More generally we define the **dihedral group** of order $2n$, for any positive integer n, as

$$\mathbf{D_{2\mathit{n}} = \langle A^{\mathit{n}}, B^2, BA = A^{-1}B\rangle.}$$

It gets the name ‘dihedral’ (literally ‘two faces’) from the fact that it’s the rotation group of an n-sided regular polygon.

Representing a group in terms of generators and relations is not a new concept, but it has becoming increasingly important over the last few years and it’s a further level of abstraction in group theory. All the information needed to compute in this group is inherent in the relations. Many groups that arise in applications come in this form. A huge amount of recent work has gone into extracting the properties of a group from such a presentation. More of this later.

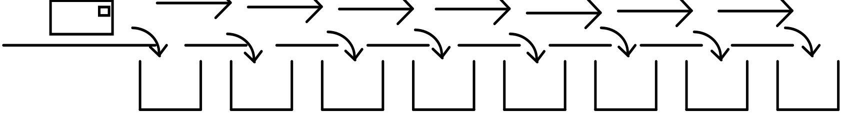
For now, let's get back to the dihedral group of order 8. It's just one of the infinitely many groups that exist, but it's one that keeps popping up in applications. We met it as the rotation group of the square but in the next three sections we'll find it arising in the context of mail sorting, the kinship rules of a certain tribe of First Nation People in Australia and the basis for a children's party game.

"But that's not mathematics!" you may be thinking. Hopefully, as a result of learning some group theory, you'll have a better appreciation of what mathematics is. It's not just about counting or measurement. It's also about patterns and rules and structure.

§1.4. Groups and Mail Sorting

These days letters are sorted by machine. The postage stamp is, or should be, in the top right-hand corner but most letters will come into the sorting machine upside-down or back-to-front. So the machine has to orient all the letters in the same way.

Suppose the letters are coming in on a conveyor belt in all possible orientations. We can have a detector, which scans the top right-hand corner for a stamp. Those envelopes whose stamp is detected are sent off for further processing and the rest are rotated in some way.



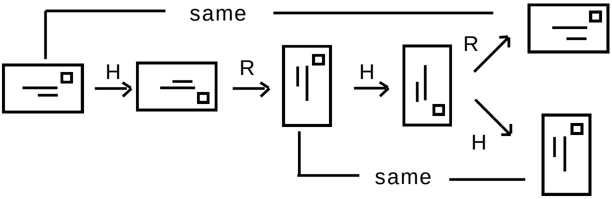
From here they pass to another detector, and so on. In this way a given letter can be flipped over and rotated until a stamp is detected. And any letter, for which no stamp can be found, goes off to another place.

Even though most letters are rectangular rather than square the possible flips and rotations will all be elements of the rotation group of a square – the dihedral group of order 8.

Two operations that are widely used in mail sorting machines are R = a 90° anti-clockwise rotation and H = a horizontal flip (top to bottom). These are the two generators A and B of the dihedral group under different names. Although, in theory, a left-to-right flip could be used, it's only in recent years that such flips have been possible at high speed. And flips about a diagonal seem to be quite impractical to implement.

Now it's obvious that a system involving eight detectors and seven flip/rotation operations is necessary. (We don't need a machine to produce the identity rotation!) And since it's reasonable to want to minimize the number of operations, we should limit ourselves to just seven. But not every sequence of 7 H's and R's will achieve the desired result of putting a letter through all 8 possible orientations.

Obviously it would be no good having two successive H's or four R's in a row. And while it might have been patriotic for the British Post Office to start the sequence with HRH, the next step would be forced to repeat an orientation that has already occurred. This is because HRH is equivalent to R^3 and so if the next operation was R the letter would repeat its original orientation while if it was H we would repeat the orientation we had two steps before.



Less obviously, the sequence RRHRRHR will not do because it repeats two orientations while missing out two others. (Check this yourself.)

A letter-facing sequence that is actually used is RRRHRRR. (Check that this achieves all eight orientations.) The sequence RRHRRRH is also used.

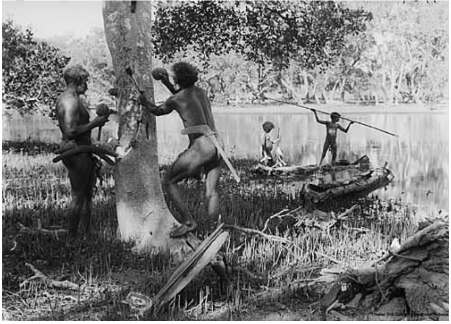
Mathematically these are equally good solutions to the problem. But according to Post Office engineers [**G.P. Copping**: *Automatic Letter Facing, British Postal Engineering*, **Proceedings of the Institution of Mechanical Engineers** (1969-70)] a horizontal flip is faster than a 90° rotation.

So it would appear that a sequence such as RRHRRRH which involves two H's and only five R's is better than one requiring one H and six R's. However one must take into account the fact that the number of letters needing to be rotated decreases as those whose stamps are detected are filtered out. So the sequence HRRRHRR, although involving the same number of each type of rotation as the one above, has fewer letters, on average, needing to be rotated by an R and so would be more efficient.

[An excellent treatment of this application can be found in **J.A. Gallian** *Group Theory and Design of a Letter Facing Machine*, **American Mathematical Monthly** vol 84 (1977) 285-287]

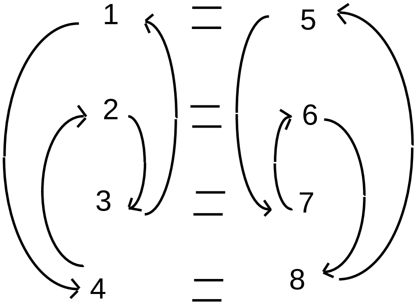
§1.5. Groups and the Kinship System of the Warlpiri Tribe

The traditional lands of the Warlpiri people lies to the north west of Alice Springs in Australia. It's incredible that such a sophisticated concept as the dihedral group of order 8 should have existed among such people for thousands of years. Of course it's misleading to suggest that they knew the abstract concept itself. However D_8 is certainly the correct model to explain the complex rules concerning intermarriage within this tribe.

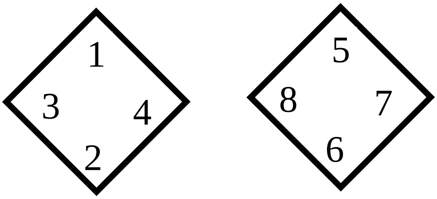


Moreover anthropologists have discovered that members of the tribe were able to rapidly perform the necessary calculations required to decide whether or not a given marriage could be allowed – calculations that are equivalent to performing arithmetic in D_8.

The Warlpiri tribe is divided into eight kinship groups, which we shall name as 1, 2, ... 8. These eight groups are paired: (1, 5), (2, 6), (3, 7), (4, 8) and the rules involve a diagram such as the following (they would actually draw diagrams in the sand while explaining their rules to the anthropologists):



The equal signs show the marriage rules. A man from group 1 could only marry a woman from group 5, and so on. The arrows point from a mother's group to her child's. So any children born to a marriage between a group 1 man and a group 5 woman, was considered to be in group 7. A boy in this family could only marry a group 3 woman and their children would be in group 1.



The Warlpiri people didn't have cards, but if they did they might have used a square card and numbered the corners 1 to 4 on one side and 5 to 8 on the other as in this diagram. Each picture shows what happens if you flip the other about the vertical axis.

These cards could be used as a tool in making kinship calculations as follows. Hold the card with your own group facing you at the top. To see whom you can marry, flip the card about the vertical axis.

Your spouse's group is now at the top. If you are a mother you can find which group your children belong to by holding the card so your tribe number is at the top and rotating the card anti-clockwise through 90°. Their kinship group now appears at the top.

It's clear from this that the kinship rules operate according to the arithmetic of D_8. Let C be the rotation through 90° about the vertical axis, reflecting the child rule, and let M be the rotation through 180° about the vertical axis. Then the group is:

$$\langle C, M \mid C^4, M^2, MC = C^{-1}M\rangle.$$

So from the fact that $C^4 = 1$, a woman is always in the same group as her maternal great-great grandmother, a fact well-known to the tribe. A man is always in the same group as his paternal grandfather, reflecting the fact that $(MC)^2 = 1$. And a woman's mother-in-law is in the same group as her daughter-in-law since

$$MC^{-1} = CM.$$

[This application is discussed in a book by **Marcia Ascher** *Ethno mathematics: A multicultural View of Mathematics*, Belmont, California: Brooks-Cole (1991) reviewed by **Judith Grabiner** in the **American Mathematical Monthly** March 1993.]

§1.6. *Galois Says* (A Children's Party Game)

An amusing application of group theory is to a children's party game called *Galois Says*, in memory of Évariste Galois who created group theory before he was killed in a duel at the age of 20. It's a rather fun sort of game that can be counted on to keep a bunch of bored children amused – for a few minutes anyway. Who says mathematics can't be useful!

Galois Says is a game basically like *O'Grady Says* where players are 'out' if they make a mistake in obeying the leader's instructions. These instructions refer to a duel with loaded pistols.

The instructions are RIGHT, LEFT and LOAD. With RIGHT and LEFT you simply do the appropriate right or left turn. To LOAD, you hold your hand up with two fingers outstretched as if holding a pistol. Now here's the catch.

*Whenever the gun is loaded you must do the **opposite** to what you are told.*

If your gun is loaded and you're told to load, you must **unload**, that is, fire. You pretend to fire the gun and your hand drops to your side. If told to turn right with a loaded gun you must turn left and vice versa. But only when the gun is loaded do you do the opposite. At other times you must obey the instructions exactly. It’s quite hilarious to watch when a number of people are playing and you really need to keep your wits about you to play well.

The game is a manifestation of the dihedral group of order 8. The instruction RIGHT is equivalent to the generator A, the instruction LEFT is equivalent to A^{-1} and the instruction LOAD is equivalent to B. Just as we got $AB = BA^{-1}$ so in *Galois Says*,

$$\text{RIGHT} \times \text{LOAD} = \text{LOAD} \times \text{LEFT}.$$

§1.7. Galois and His Groups

The day you began to learn group theory should be recorded in your diary as a red-letter day because it represents that point in your mathematical education when you began to think at a new level of abstraction. And on the historical level the discovery of groups marked one of the three or four major changes of direction in the whole history of mathematics.

Although some vague ideas connected with groups were around a little earlier, without doubt the honour of being the founder of group theory goes to Évariste Galois, a young Frenchman who was fascinated by the inability of mathematicians to discover a formula for solving quintics (polynomial equations involving powers of x up to x^5). The type of formula they were looking for was one like the quadratic formula which finds the solutions in terms of the coefficients using the operations of addition, subtraction, multiplication and division and radicals (the extraction of roots – square roots, cube roots etc).

A formula for the cubic was found in 1515 and the quartic was solved in 1545. The next step was the solution of the general quintic. It wasn't until the early part of the nineteenth century that the Norwegian mathematician, Abel, proved that such a formula doesn't exist.

Of course there are numerical techniques, which essentially enable us to solve any polynomial equation to any desired degree of accuracy. If you've met Newton's Method you will probably nod your head in agreement. But I should point out that it's not that easy. For a start Newton's Method can only deal with polynomials with real coefficients. And even if you have a real polynomial Newton's Method will only find its real zeros. How would you go about solving a real polynomial of degree 6 if the zeros consisted of three conjugate pairs? You can find a generalization to Newton's Method that handles complex zeros in my notes on *Galois Theory*.

But what if we want an *exact* formula of the type described above. For a general quintic (or polynomial of higher degree) such a formula will never be found because Abel proved that it is logically impossible.

Now Galois knew of Abel's work but he wanted to go a stage further. He noted that some quintics *are* soluble by radicals, that is, their **zeros** (values of *x* that make the polynomial equal to zero) *can* be expressed exactly by a formula of the above type. But for others it isn’t possible. Which ones are soluble by radicals and which are not?

Galois studied algebraic expressions involving the zeros α, β, γ, δ, ... of a polynomial. Certain permutations of the zeros always leave the value of these expressions unchanged. For example, in the case of $E = \alpha\beta + \gamma\delta$, one could swap α and β or swap γ and δ, or perform both swaps together, and the value of E will be unchanged. Or the pairs (α, β) and (γ, δ) themselves could be interchanged. A less obvious permutation would be:

$$\alpha \to \gamma \to \beta \to \delta \to \alpha.$$

This permutation transforms E into the expression $\gamma\delta + \beta\alpha = E$ and so leaves the value of E unchanged. There are, in all, 8 permutations of the set $\{\alpha, \beta, \gamma, \delta\}$ which leave the value of E unchanged and these form the dihedral group D_8.

Other expressions have less symmetry. For example, if $F = \alpha\beta - \gamma\delta$ the only permutations that leave F unchanged, apart from the identity, are swapping α and β, swapping γ and δ and their product which consists of swapping the elements of both pairs.

An expression that is less symmetrical again is $G = \alpha\beta + \gamma - \delta$, while $H = \alpha + \beta\gamma^2\delta^3$ is only fixed by the identity permutation.

Galois associated with every polynomial a group (now called its ‘Galois group’) which consists of certain permutations of the zeros. He then described the solubility by radicals (the existence of a formula like the quadratic, cubic and quartic ones), of such a polynomial in terms of the structure of its group.

The life of Galois is just as fascinating as his work. It was once the subject of a full-length feature film and in 1998 the biography *The French Mathematician* was published as a paperback.

Galois didn’t do very well at school. He got involved in student political riots, he did much of his mathematics during his frequent spells in prison and he tried unsuccessfully to get the established mathematical community to take notice of his work. He was killed in a duel. All before the age of twenty-one! An account of his life is given in one of the appendices of these notes.

EXERCISES FOR CHAPTER 1

EXERCISE 1: For each of the following statements determine whether it is TRUE or FALSE.

(1) One of the group axioms is the commutative law:

$$a * b = b * a \text{ for all } a, b.$$

(2) A group is a set that is closed under an associative binary operation that has an identity and where every element has an inverse.

(3) If A, B, C are the three rotations in the Dutch Wife's Mattress Problem (see §1.2) then ABC = I.

(4) If A, B are the rotations described in §1.3 then

$$(AB)^2 = I.$$

(5) There are exactly 5 solutions to the equation $x^2 = I$ in the dihedral group D_8.

(6) The sequence of operations HRHHRRR is a letter-facing sequence (see §1.4) – that is, if letters are scanned in the top-right-hand corner and are rotated according to this sequence then all letters with a stamp in one of the 8 corners will have that stamp detected.

(7) If you begin by facing North with your gun unloaded, in the game *Galois Says* (see §1.6) and obey the following sequence of instructions LOAD, LEFT, LOAD, RIGHT you will end up facing South with your gun unloaded.

(8) Swapping α, β leaves the expression $E = (\alpha - \beta)^2$ unchanged.

(9) Galois died of old age.

(10) Abstraction is a powerful tool in mathematics.

EXERCISE 2: If A, B, C represent the three mattress-turning operations and the sequence ABACACBABAA is carried out month by month over an 11 month period, what operation should be carried out in the 12th month in order for the mattress to return to its original position at the end of the 12 months?

EXERCISE 3: Show that if the sequence of operations ABACACBABAAB is carried out, month by month over a twelve month period, the mattress will be in each of its four possible positions for exactly 3 of the 12 months.

EXERCISE 4: Suppose you have an equilateral triangle and A represents the rotation through 120° in an anticlockwise direction about the centre of the triangle, and suppose that B represents a 180° rotation about an axis of symmetry. Prepare a multiplication table for the group generated by A, B.

EXERCISE 5: If you start playing *Galois Says* facing West with the gun loaded and you are told LEFT, which direction should you now be facing?

EXERCISE 6: In playing *Galois Says*, show that:
LEFT × LOAD × RIGHT = RIGHT × LOAD × LEFT.

EXERCISE 7: In how many different ways can you write the algebraic expression $abc + def$ so that its value is unchanged. (For example, $fde + bac$ has the same value as $abc + def$ even though it looks different. Include the expression $abc + def$ itself.)

EXERCISE 8: Show that the operation: $\alpha \rightarrow \gamma, \beta \rightarrow \delta, \gamma \rightarrow \beta, \delta \rightarrow \alpha$ leaves the value of the expression $\alpha\beta + \gamma\delta$ unchanged while the operation:

$$\alpha \rightarrow \beta, \beta \rightarrow \gamma, \gamma \rightarrow \delta, \delta \rightarrow \alpha$$

does not.

EXERCISE 9: Consider the set G = {A, B, C, D} under the binary operation given by the following table:

*	I	A	B	C
I	I	A	B	C
A	A	B	C	A
B	B	C	A	I
C	C	I	I	B

Calculate two different values of A^4, by putting parentheses into $A * A * A * A$ in different ways. So the associative law does not hold. Which of the other 3 group axioms hold for this system? Is this an abelian group?

SOLUTIONS FOR CHAPTER 1

EXERCISE 1:
(1) is FALSE – the commutative law only holds in abelian groups;
(2) TRUE;
(3) TRUE, since AB = C and $C^2 = I$;
(4) TRUE;
(5) FALSE – there are 6 solutions: I, A^2, B, AB, A^2B and A^3B
(6) FALSE, because HH = I;
(7) TRUE;
(8) TRUE;
(9) FALSE – he was killed in a duel at 20;
(10) TRUE

EXERCISE 2: Since the commutative law $xy = yx$ holds in the mattress group we can simplify ABACACBABAA to $A^6B^3C^2 = B$, so an extra factor of B is required to make the product the identity.

EXERCISE 3: The successive products after 1, 2, 3, … months are:
A, AB = C, ABA = CA = B, ABAC = BC = A, etc.

These products are A, C, B, A, I, C, A, I, B, C, B, I. Each of these represents one of the four positions of the mattress and each occurs 3 times.

EXERCISE 4:

	I	**A**	**A^2**	**B**	**AB**	**A^2B**
I	I	A	A^2	B	AB	A^2B
A	A	A^2	I	AB	A^2B	B
A^2	A^2	I	A	A^2B	B	AB
B	B	A^2B	AB	I	A^2	A
AB	AB	B	A^2B	A	I	A^2
A^2B	A^2B	AB	B	A^2	A	I

EXERCISE 5: NORTH (that is you turn right because the gun is loaded).

EXERCISE 6: If you start facing North, for example, with the gun unloaded then LEFT × LOAD × RIGHT and RIGHT × LOAD × LEFT both result in you facing South with the gun unloaded. There's a difference in how you got there (in one case you'll have made two left turns and in the other you'll have made two right turns) but we're only taking into account the final position, which is the same in each case.

EXERCISE 7: There are 6 ways of arranging *a*, *b*, *c* and for each of these there are 6 ways of arranging *d*, *e*, *f*. So in all there are 36 ways of writing *abc* + *def* in such a way that the first term is equivalent to *abc*.

But the two terms can be swapped, giving twice as many possibilities altogether, that is, there are 72 ways of writing *abc* + *def*.

EXERCISE 8: The first operation changes $\alpha\beta + \gamma\delta$ into $\gamma\delta + \beta\alpha$ which algebraically is equivalent to $\alpha\beta + \gamma\delta$. The second operation changes $\alpha\beta + \gamma\delta$ into $\beta\gamma + \delta\alpha$ which is equivalent to $\alpha\delta + \beta\gamma$ but not the original expression $\alpha\beta + \gamma\delta$.

EXERCISE 9: $(A * A) * (A * A) = B * B = A$ while

$$((A * A) * A) = (B * A) * A = C * A = I.$$

(All the other ways of inserting parentheses also give I. This system satisfies the Closure Law, the Identity Law and the Inverse Law. It even satisfies the Commutative Law. But, without the Associative Law it is not a group.