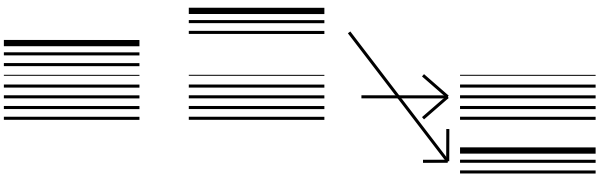
2. PERMUTATIONS

§2.1. Shuffling a Pack of Cards

What we're attempting to do when we shuffle a pack of cards is to put them in a random order and this assumes that we're unable to keep track of what we're doing. But many magicians, and no doubt many card sharps, learn to be in complete control of their shuffling. They carry out a number of basic steps in quick succession, each of which rearranges the cards. While each individual step has a very simple effect, the overall effect can be quite complicated.

Suppose we were able to shuffle in a very precise and controlled way. If we knew the initial order of the cards and we recorded our movements we'd be able, in principle, to predict the final order of the cards. But to do this efficiently we'd need a system of notation to describe the different shuffling operations.

A basic shuffle is to cut the deck. This means taking n cards off the top and putting them on the bottom. An experienced card shuffler is able to control the value of n, without appearing to count.



To keep things simple let's work with a pack of 8 cards, numbered 1 to 8. You should make your own pack and carry out the various shuffles. At the beginning of each shuffle or sequence of shuffles we 'reset' the pack by putting the cards in order, 1 at the top and 8 at the bottom.

Let C_n denote the operation of cutting the cards by taking off the top n cards and putting them on the bottom. The effect of each of these is as follows.

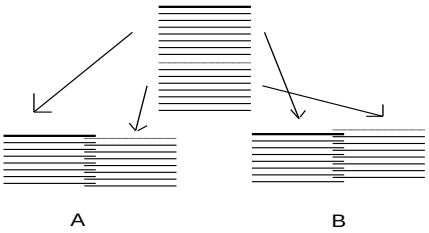
	C_1	C_2	C_3	C_4	C_5	C_6	C_7
1	2	3	4	5	6	7	8
2	3	4	5	6	7	8	1
3	4	5	6	7	8	1	2
4	5	6	7	8	1	2	3
5	6	7	8	1	2	3	4
6	7	8	1	2	3	4	5
7	8	1	2	3	4	5	6
8	1	2	3	4	5	6	7

Note that C_n can be achieved by repeating C_1 a total of n times – transferring n cards in one go is no different to transferring them one at a time. And the simplest way to achieve C_7 is to take the bottom card and put it on top, rather than take the top seven cards and putting them on the bottom. In fact C_7 and C_1 are inverses of one another.

Another basic shuffle is to cut the pack, assuming the number of cards is even, into two equal stacks. Place these two stacks next to one another and ruffle them so that they fall alternately into one stack. An experienced

card shuffler can do this accurately and effortlessly, so that the cards are exactly interleaved. The effect may look random but done by a professional the effect can be completely predictable.

A simpler, though less impressive, way to achieve this result is to alternately pick up one card from each half stack. But there are two variations to this shuffle, depending on whether the top card after the ruffle was the top card of the left or the right half pack, that is, whether it was the top card of the whole deck or the top card of the bottom half. Let's denote these two shuffles by A, B respectively.



Again we'll illustrate this for a pack of 8 cards. The effect of performing these ruffles is as follows:

	A	**B**
1	1	5
2	5	1
3	2	6
4	6	2
5	3	7
6	7	3
7	4	8
8	8	4

§2.2. Multiplying Shuffles

There are other basic types of shuffle but these will do for now. We're going to analyse the effect of performing a sequence of basic shuffles and what we need is an arithmetic of shuffles. The effect of performing one shuffle after another we'll call their **product**. Of course multiplication of shuffles has nothing to do with multiplication of numbers, but it's a useful analogy.

The fact that C_3 is equivalent to doing C_1 three times in succession can be expressed very simply by the equation $C_3 = C_1^3$. In fact all the cut operations can be expressed in terms of C_1. So if we write C_1 as just C, we can say that $C_n = C^n$.

So far we've considered three basic shuffling operations:

A = interleave the top half with the bottom half so that the top card remains on top;

B = interleave the top half with the bottom half so that the top card of the bottom half ends up on top;

C = take the top card and put it on the bottom.

What's the effect of doing $A^2B^3C^4$? This means doing A twice, then doing B three times, and finally doing C four times. At this stage the only way you'll be able to work it out is to actually perform the shuffles with your pack of cards.

Prepare eight cards, numbered 1 to 8, and arrange them in order with 1 on top and 8 on the bottom. Now carefully perform $A^2B^3C^4$. If you've done it correctly the order of the cards should now be: 7, 5, 3, 1, 8, 6, 4, 2.

It would be nice to be able to calculate the result without having to carry out the experiment. When you've learnt more about the theory of permutations you'll be able to do this.

Permutations are just ways of rearranging a set of objects. When the objects are cards we call them 'shuffles'. We multiply permutations by performing them in succession and in some ways the multiplication of permutations behaves like the multiplication of numbers.

For numbers it is the case that $(xy)z = x(yz)$. This is also true for permutations. Each of these products is simply the effect of doing x, then y, then z.

Numbers also satisfy $xy = yx$. It makes no difference whether one multiplies 3×5 or 5×3. The answer is 15 in both cases. But for permutations you usually get a different answer if you multiply them in a different order.

To see this use your 8 cards. Put them in order. Now carry out operation A, then B. The final order of the cards should be 3, 1, 7, 5, 4, 2, 8, 6. Now return the cards to their original order and this time do B first and then A. This time 5 is on top and the order of the cards is 5, 7, 1, 3, 6, 8, 2, 4. The two products are different: $AB \neq BA$.

Permutations have to do with changing the order of things and, as we've seen, the order in which we multiply permutations is important. (Here I'm using the word 'order' in its usual, non-technical sense. The word 'order' is used in group theory in a technical sense to describe the size of a group or the smallest power of an element of a group that produces the identity.) To illustrate this concept we'll carry out another experiment with our 8 cards.

Put them in their correct order and carry out the operation A. The order of the cards should now be 1, 5, 2, 6, 3, 7, 4, 8. Now carry out operation A again. The cards should now be in the order 1, 3, 5, 7, 2, 4, 6, 8. Now carry out operation A for a third time. This time the cards should have returned to their original order: 1, 2, 3, 4, 5, 6, 7, 8.

We use the symbol I to represent the permutation that leaves everything where it is. You might object that this is not really a rearrangement. But just as 0 is a very useful number, even though it counts nothing at all, the so-called **identity permutation I** is extremely useful.

We can sum up the result of our experiment by saying that $A^3 = I$. Using the word 'order' in its technical sense in group theory we can say that "A has order 3". The **order** of a permutation is the least number of times you need to perform it for everything to return to its original position.

You may remember that we called the size of a group its order. The **order** of an element *x* is the smallest

positive integer n such that x^n is the identity. The order of a group is its size. These are two different things though, as we will see later, they are closely related.

Clearly, with 8 cards, C has order 8, because when taking one card off the top and putting it on the bottom, you need to do it 8 times before everything is back where it started.

What's the order of B? Return the deck of 8 cards to their original position and carry out B repeatedly. After three times you should still be going. It will take six performances of B altogether before the cards return to their natural order. In other words, B has order 6.

We've introduced an efficient way of representing complicated permutations in terms of simpler ones but as yet we don't have an efficient notation for those basic operations. Up till now we've had to resort to carefully worded descriptions of how to carry out the permutations A, B and C with an actual pack of cards. What we need next is a compact symbolic notation to describe the effect of a permutation. Then we can begin to develop computational techniques for multiplying them.

§2.3. Permutations

When you learnt about permutations and combinations you were learning to count arrangements. You called them 'permutations', and in normal life we call them 'permutations', but the correct mathematical term is 'arrangement'. An **arrangement** of a finite set is a list of its elements in a particular order. A **permutation**

is an operation of changing one arrangement into another (or, in the case of the identity permutation, leaving the arrangement the same). Altogether there are $n!$ arrangements of a set with n elements.

The 24 arrangements of the set {1, 2, 3, 4} are:

1234	1243	1324	1342	1423	1432
2134	2143	2314	2341	2413	2431
3124	3142	3214	3241	3412	3421
4123	4132	4213	4231	4312	4321

A pack of cards gives an arrangement of the set of 52 cards. Shuffling the pack changes the arrangement. The card that was previously in position 1 (say, the top card) might now be in position 23, the card that was in position 2 might now be in position 42, and so on.

If we started with the pack in some specific order and took the top 10 cards and put them on the bottom – that is, if we cut the deck after the 10th card – we could record the change of arrangement as follows:

card that was in position →	1	2	...	10	11	...	52
is now in position →	43	44	...	52	1	...	42

This table defines a function from the set:

$$S = \{1, 2, 3, \ldots, 52\}$$

to itself. If $f: S \to S$ denotes this function then $f(1) = 43$; $f(2) = 44$; etc.

Notice that we consider the permutation as acting on the set of *positions* rather than on the set of *cards*. This is because a given shuffling operation, such as taking the top ten cards from the top to the bottom of the pack, is independent of which cards they are. The top ten cards are not the same every time, but the positions are.

Not every function on a set can describe a change of arrangement. For example the function given by the following table can't.

n	1	2	3	4	5
$f(n)$	4	3	1	3	2

This is because two cards would have to occupy the 3rd position, and no card is in 5th position even though there are 5 cards.

Only a function that's 1-1 (different elements map to different elements) and onto (every element is mapped to) can describe a rearrangement.

A **permutation** on a set S is a 1-1 and onto function from S to itself. There are permutations on infinite sets (eg. the function f: $\mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^3$ is a permutation on $\mathbb{R}$, the set of real numbers) but we generally confine our attention to finite sets, and generally sets of numbers such as $\{1, 2, 3, ..., n\}$. We denote the set $\{1, 2, 3, ... , n\}$ by $\mathbf{[n]}$.

Don't confuse an *arrangement* with a *permutation*. An arrangement is a static thing while a permutation is dynamic. It is a *re*-arrangement, something that changes one arrangement to another. But since the bottom row of the function table of a permutation on a finite set is an arrangement, there are exactly as many permutations as there are arrangements, namely $n!$ for a set with n elements. The set of all permutations on the set $[n]$ is called the **symmetric group** of degree n and is denoted by $\mathbf{S}_n$.

§2.4. Cycle Notation

The simplest way to represent a permutation on a finite set is to set up a table of values such as:

x_1	x_2	...	x_n
$f(x_1)$	$f(x_2)$	…	$f(x_n)$

Often this is written as: $\begin{pmatrix} x_1 & x_2 & \dots & x_n \\ f(x_1) & f(x_2) & \dots & f(x_n) \end{pmatrix}$.

For example $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 6 & 4 & 2 & 1 \end{pmatrix}$ represents a permutation, f, on the set [6] defined by:

$f(1) = 3$; $f(2) = 5$; $f(3) = 6$; $f(4) = 4$; $f(5) = 2$; $f(6) = 1$.

Starting with the arrangement 1 2 3 4 5 6 this results in the arrangement 6, 5, 1, 4, 2, 3 because what was previously in position 6 is now in position 1, what was in position 5 is now in position 2, and so on.

Another system is to use arrows to denote the images of the elements, such as:

$$1 \to 3$$
$$2 \to 5$$
$$3 \to 6$$
$$4 \to 4$$
$$5 \to 2$$
$$6 \to 1$$

A more compact system is to write them all on one line:

$$1 \to 3;\ 2 \to 5;\ 3 \to 6;\ 4 \to 4;\ 5 \to 2;\ 6 \to 1.$$

.

The order of each piece of information is irrelevant and so the function could have been written as: $1 \to 3;\ 3 \to 6;\ 6 \to 1;\ 2 \to 5;\ 5 \to 2;\ 4 \to 4$
or more simply as: $1 \to 3 \to 6 \to 1;\ 2 \to 5 \to 2;\ 4 \to 4$

Here we've broken the permutation into disjoint cycles. In this example there are three cycles, of lengths 3, 2 and 1 respectively.

An even more compact notation is to write it as:

$$(1\ 3\ 6)(2\ 5)(4).$$

The convention is that each symbol is mapped to the one on the right except the last, which is mapped to the first. We can make the notation more compact still by one further convention. If it's clear on what set the permutation is operating we may omit cycles of length 1. So (1 3 6)(2 5)(4) can be abbreviated to just (1 3 6)(2 5).

Any symbol that's not present is assumed to be fixed (that is, mapped to itself).

There's just one tiny problem with this. The identity function fixes *every* symbol and if we omitted cycles of length 1 we'd have a blank space! For the special case of the identity permutation we use the symbol I.

Example 1: The function f: [8] $\rightarrow$ [8] defined by:

$$f(1) = 2,\ f(2) = 7,\ f(3) = 4,\ f(4) = 3,$$
$$f(5) = 8,\ f(6) = 6,\ f(7) = 1,\ f(8) = 5$$

is a permutation. In cycle notation it's written:

$$(1\ 2\ 7)(3\ 4)(5\ 8).$$

What is the corresponding arrangement if we begin with

$$1, 2, 3, 4, 5, 6, 7, 8?$$

The answer is: 7, 1, 4, 3, 8, 6, 2, 5. Remember that if $f(x) = y$ then what was previously in position x is now in position y. It does *not* mean that card labelled x is in position y.

Example 2: If f is the permutation denoted by the cycle notation (1 9 4 6)(2 5 3) this means that $f(9) = 4$ (next on right), $f(3) = 2$ (last in cycle maps to first); $f(7) = 7$ (omitted symbols are fixed).

The system of notation just described is called **cycle notation**. It reveals a good deal about the structure and properties of a permutation – much more easily than with a table of values.

CYCLE NOTATION RULES

(1) The numbers represent *positions* not what is currently in that position.
(2) Each symbol is mapped to the one on its right except the last in each cycle which is mapped to the first.
(3) Fixed symbols (cycles of length 1) are omitted.
(4) The identity permutation is denoted by I.

In addition to these rules there are some optional conventions. For a start, if the symbols are single digits we may omit the spaces between them and so write (123) instead of (1 2 3).

The same permutation can be written in several different ways. For example

(12345) = (23451) = (34512) = (45123) = (51234).

It's only the cyclic order that matters and so the symbols in any cycle may be permuted cyclically to bring any one of them to the front. If the symbols are positive integers we generally bring the smallest to the front. So, although it isn't wrong to write (31254), the preferred notation would be (12543).

The cycles in the cycle notation are 'disjoint', that is, they have no symbols in common. For this reason they're independent from one another and may be rearranged in any order (as whole blocks). For example (376)(18)(2549) = (2549)(18)(376) = (376)(18)(2549) etc. We sometimes adopt the convention that cycles are

arranged in order of their first symbol, writing the above as (18)(2549)(376).

CYCLE NOTATION CONVENTIONS (Optional)
(1) Spaces are omitted where there's no ambiguity (eg. single digits).
(2) The smallest symbol in each cycle is brought to the front.
(3) The cycles in a given permutation are arranged in ascending order of their first symbols.

Using these optional conventions, each permutation has a unique description.

§2.5. Cycle Structure

A cycle of length n is called an ***n*-cycle**. (Often 2-cycles are called **transpositions**.) The **cycle structure** of a permutation is its structure as a collection of disjoint cycles and it's expressed by replacing the symbols by ×'s. (The cycle structure of I is I itself.) For example, the cycle structure of (15)(243)(59) is (××)(×××)(××). Since we can no longer arrange the cycles in order of their first symbols, we generally arrange them in order of their lengths so that we would write the above cycle structure as (××)(××)(×××).

The cycle structure of a permutation reveals a lot about its properties. Permutations having the same cycle structure have much in common as we'll see. Let's now

use cycle structure to systematically explore the groups $\mathbf{S}_1$, $\mathbf{S}_2$, $\mathbf{S}_3$ and $\mathbf{S}_4$.

THE SYMMETRIC GROUP $\mathbf{S}_1$

Shuffling a pack of 1 card isn't very interesting! The only permutation in $\mathbf{S}_1$ is the identity, I.

THE SYMMETRIC GROUP $\mathbf{S}_2$ Things aren't much better with 2 cards, but at least we can swap them.
$S_2 = \{I, (12)\}$.

THE SYMMETRIC GROUP $\mathbf{S}_3$

Here's where things start to get interesting. The possible cycle structures are: I, $(\times\times)$ and $(\times\times\times)$. With a 2-cycle $(\times\times)$ there are $3 \times 2 = 6$ ways of replacing the $\times$'s by two distinct elements of [3], namely (12), (13), (21), (23), (31), (32). But (21) = (12) and so on, so we only get 3 distinct 2-cycles, not 6: (12), (13), (23).

Similarly while there are $3 \times 2 \times 1 = 6$ distinct symbols of the form $(\times\times\times)$ we again get repetitions. Since the smallest symbol in a cycle can be brought to the front we must divide by 3 in this case. So there are thus just two 3-cycles in $\mathbf{S}_3$ viz. (123) and (132).
Hence $\mathbf{S}_3 = \{I, (12), (13), (23), (123), (132)\}$.

THE SYMMETRIC GROUP $\mathbf{S}_4$

The possible cycle structures on 4 symbols are:
I, $(\times\times)$, $(\times\times\times)$, $(\times\times\times\times)$ and the double 2-cycle $(\times\times)(\times\times)$.

There is of course only one identity permutation. We get the number of 2-cycles by considering the fact that there are $4 \times 3 = 12$ ways of filling in the ×'s in (××) but since either symbol may be brought to the front, we must divide by 2. There are thus 6 cycles of length 2. The number of 3-cycles is $\frac{4 \times 3 \times 2}{3} = 8$ and there are $\frac{4 \times 3 \times 2 \times 1}{4} = 6$ cycles of length 4.

The calculation is slightly more complicated when we come to the double 2-cycles. There are 4! = 24 ways of replacing the ×'s by symbols in (××)(××). Of course we must divide by 2 for each 2-cycle to take account of the fact that $(a\ b) = (b\ a)$. But, in addition, we must divide by a further factor of 2 because of the fact that

$$(a\ b)(c\ d) = (c\ d)(a\ b).$$

The number of double 2-cycles is thus: $\frac{4 \times 3 \times 2 \times 1}{2 \times 2 \times 2} = 3$.

As a check we note that $1 + 6 + 8 + 6 + 3 = 24$.
The elements of $\mathbf{S}_4$ are thus:

I	(12)	(13)	(14)	(123)	(132)
(12)(34)	(23)	(24)	(34)	(124)	(142)
(13)(24)	(1234)	(1324)	(1423)	(134)	(143)
(14)(23)	(1243)	(1342)	(1432)	(234)	(243)

§2.6. The Prisoner Problem

There's a curious problem that's recently been drawn to my attention. It's based on the simple fact that every permutation is a product of cycles.

There were ten prisoners in one large cell. Each had his prison number tattooed on his arm. One day the prison warden came to them and offered them a chance to be released.

"I'm going to offer you the chance of freedom. In the next room there are ten boxes, numbered from 0 to 9. There are ten cards each containing a different digit and each card will be randomly put into one of the boxes."

"Tomorrow morning each of you will come, one at a time, and you'll be allowed to open any five of the boxes. If you find the card that contains the last digit of your prison number you'll be given a green card. Otherwise you'll get a red card."

"After you've received your card you'll be sent to another room so that you can't communicate with those that are left. Once you've all been given a card the outcome will be as follows. If everybody has a green card you'll all be released. But if one or more has a red card, you'll all be shot!"

That night they discussed what their chances were of being released.

"It's pretty hopeless," said one of them. "We each have one chance in two of finding our own card. But for

all ten of us to find our own card the probability is less than one in a thousand. We're all going to die!"

"Not necessarily," said another prisoner. "I happen to have studied group theory and I can suggest a way that will improve our chances dramatically."

"It's worth trying. What would be our chances if we followed your strategy?"

"Only about one in three, I'm afraid. But it's a lot better than one in a thousand."

"So what do we have to do?" asked another.

"When you go into the next room tomorrow, look for the box with the last digit of your prisoner number. Open that box and the card inside will give you the number of the next box to open. Keep going until you return to the box you started with. The card that took you there will have your own digit. You'll get a green card."

"Yes, but what if I look in five boxes and still don't find my number. I'd have to stop."

"And they'd give you a red card and we'd all be executed."

"And what's the chance of that?"

"About two in three. So even with my strategy we'd only have about one chance in three of getting out alive."

"That's worse than choosing randomly where it's one in two."

"Ah, but this probability won't depend on our choices. It will depend on how the cards have been

allocated. You won't have to multiply one third ten times."

"How so?"

"Well the cards in the boxes give a permutation on the ten digits. Now every permutation is a product of cycles. Suppose that all the cycles have length five or less. Then everybody will get back to their own card by opening no more than five boxes. In that case we'll all get a green card and we'll all go free."

"And if there's a cycle of length six? Somebody's number is sure to be in that cycle and, if we follow your strategy, he'll not get back to his own number by opening only five boxes. It only takes one person to get a red card and we'll all be shot."

"Well, I've worked out the probabilities and the probability of there being a cycle of length six or larger is about two in three. So that gives us a chance of about one in three of getting out of here alive!"

"But what if two of us have the same last digit?"

"That would make no difference. If there were no cycles of length six or more we'd all get a green card, even if we all had the same last digit."

So they decided to follow the group-theorist's strategy and amazingly they all got green cards and were released.

"Even though the odds were still against us we still won with a probability of one in three. There must be a God," said one of them later.

Perhaps God was looking after them, though not in the way they had imagined. You see there were two prison guards assigned to the task of setting up the room and they decided to divide the cards into two groups. One had the numbers 0 to 4 and he said to the other guard, "you put yours in the back row and I'll put mine in the front. The prisoners won't notice that it's not completely random."

Now the boxes in the front row were numbered 0 to 4 and so the guards unwittingly ensured that there were no cycles longer than five.

Here's the mathematics behind the probabilities. Without a strategy the probability of each prisoner getting a green card would be ½. So the probability of them all getting green cards would be $(½)^{10} = 1/1024$.

The distribution of the cards gives a permutation, π, on $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 0\}$.
The number of cycles of length n is:

$$\frac{10.9\ldots.(10-n+1)}{n} = \frac{10!}{n(10-n)!}$$

with the reason for dividing by n being the fact that every cycle of length n can start at any of its n digits. The number of permutations *containing* a cycle of length n is: $\frac{10!}{n(10-n)!} \times (10-n)! = \frac{10!}{n}$ since the remaining $10 - n$ *digits* can be permuted in $(10 - n)!$ ways.

Let P_n be the probability of π containing a cycle of length n. If π was indeed random, as promised, then

$$P_n = \frac{10!/n}{10!} = \frac{1}{n}.$$

So the probability of π containing a cycle of length at least six is $\frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \frac{1}{10} \approx 0.6456$.

So if the cards had been distributed randomly the probability of all the prisoners being released would be approximately $1 - 0.6456 = 0.3544$, which would have given them a fighting chance. But the careless of the guards increased this probability to 1!

§2.7. Definition of Multiplication

The **product** of two permutations f, g on a set S is the composition of the two functions in the order 'first f then g'.

Note that the usual convention with **composition** is to multiply in reverse order, first g then f. So $(f \circ g)(x) = f(g(x))$, where $f \circ g$ denotes the resulting function. In the context of permutations we write the composite as fg and define it to mean that we first apply f and then g.

$$(f \circ g)(x) = f(g(x)) \text{ while } (fg)(x) = g(f(x)).$$

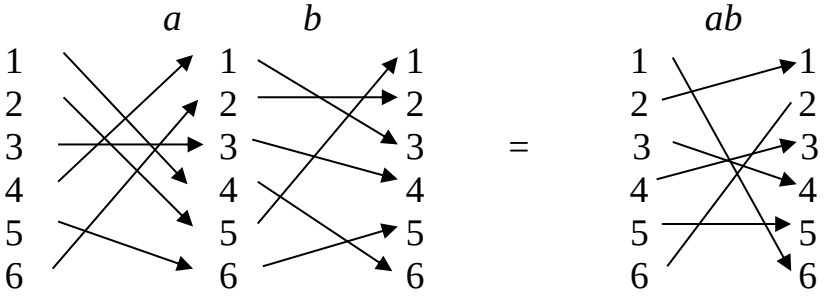
The convention for composition results from the fact that we normally write functions on the left as $f(x)$, not $(x)f$ and the definition of composition seems more natural. The $f \circ g$ notation and the accompanying convention is widely used in analysis but the left-to-right

convention of *fg* is more widespread in abstract algebra and it's the one we'll use here.

Permutations multiply in the order in which they are written, from left to right.

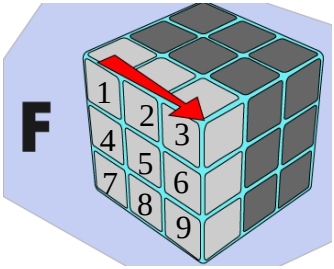
If we're given two permutations in cycle notation and we want to multiply them, we can first convert them to arrow diagrams, erase the centre column and combine each pair of arrows into a single one. Then all we have to do is to convert back to cycle notation.

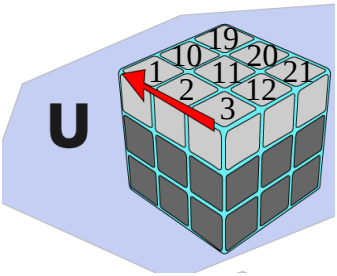
Example 3:
Suppose $a = (14)(256)$ and $b = (13465)$.
Then $ab = (162)(34)$.



But while arrow pictures can assist us when we first learn to multiply permutations they're bulky and clumsy. It's better that we learn to multiply permutations directly using cycle notation.

Numbering the 27 cubes in a Rubik's Cube systematically, F = (1 3 9 7)(2 6 8 4),
U = (1 19 21 3)(2 10 20 12),
FU = (1 19 21 3 9 7)(2 6 8 4 10 20 12 2) and $(FU)^6 = I$





§2.8. Permutation Multiplication Algorithm

The easiest way to describe the algorithm is to use it on a particular example and explain in detail what we're doing.

$$(14)(256) \times (13465) = (162)(34)$$

THINK	WRITE
1 is the first symbol in the first cycle	(1
1→4 by the first permutation then 4→6 by the second so 1→6	(16
6→2 and then 2→2 (absent so fixed) so 6→2	(162
2→5 and then 5→1 so 2→1 completing the cycle	(162)
3 is smallest symbol not yet used	(162)(3

3→3 (absent so fixed) then 3→4	(162)(34
4→1 then 1→3 completing another cycle	(162)(34)
5 is the smallest not yet used but looking ahead we see that it's fixed so we leave it out	(162)(34)
all symbols are accounted for so stop	(162)(34) is the answer

Here's a second example with a more abbreviated explanation:

(1463)(587) × (1374628) = (1675)(284)

THINK	**WRITE**
(**14**63)(587) × (137**46**28)	(16
(14**63**)(587) × (1**3**74628)	(167
(1463)(**5**8**7**) × (1374628)	(1675
(1463)(**58**7) × (**1**374628)	(1675)
new cycle	
(1463)(587) × (13746**28**)	(1675)(28
(1463)(5**87**) × (13**74**628)	(1675)(284
(1**46**3)(587) × (1374**62**8)	(1675)(284)

Example 4:

The following is the multiplication table for $\mathbf{S}_3$, the group of permutations on 3 symbols:

	I	(123)	(132)	(12)	(13)	(23)
I	I	(123)	(132)	(12)	(13)	(23)
(123)	(123)	(132)	I	(23)	(12)	(13)
(132)	(132)	I	(123)	(13)	(23)	(12)
(12)	(12)	(13)	(23)	I	(123)	(132)
(13)	(13)	(23)	(12)	(132)	I	(123)
(23)	(23)	(12)	(13)	(123)	(132)	I

§2.9. Powers of Permutations

To raise a permutation to the *m*'th power using cycle notation, simply jump forward, *m* steps at a time. (Wrap around if you go past the end of a cycle.)

Thus $(x_1\ x_2\ \ldots\ x_n)^m = (x_1\ x_{m+1}\ x_{2m+1}\ \ldots\ )$

Example 5: If a = (1426537) then a^2 = (1257463).
Think of this as:

1→4→2,
2→6→5,
5→3→7,
7→(wrap around)1→4,
4→2→6,
6→5→3,
3→7→1(wrap around).
Then ignore the intermediate stage.

Example 6:

If a = (123456789) then a^2 = (135792468)
a^3 = (147)(258)(369) a^4 = (159483726)
a^5 = (162738495) a^6 = (174)(285)(396)
a^7 = (186429753) a^8 = (198765432)
a^9 = I.

Carefully examine the pattern. For example, with a^3 we jump in steps of size 3. By the time we come to a^7 we see that it's equivalent (and easier) to count back 2 steps each time rather than 7 steps forward.

Clearly $a^{10} = a$, $a^{11} = a^2$ etc.

The inverse of $a = (x_1\, x_2 \ldots x_m)(y_1\, y_2 \ldots y_n) \ldots$ is

$$a^{-1} = (x_1\, x_m \ldots x_2)(y_1\, y_n \ldots y_2) \ldots$$

We begin each cycle at the same point as before but go around in the reverse order.

Example 7:

The inverse of (16243)(579) is (13426)(597)

For all permutations $aa^{-1} = \mathrm{I} = a^{-1}a$. This is because a^{-1} undoes whatever a achieves.

§2.10. Order of a Permutation

The **order** of a permutation a, is the smallest positive integer n such that $a^n = \mathrm{I}$.

Example 8: The order of (162) is 3. More generally, the order of an n-cycle is n.

The order of (12)(345) is 6 because for its n'th power to be the identity, n must be both even (to 'kill off' the 2-cycle) and a multiple of 3 (to 'kill off' the 3-cycle). The smallest positive integer that is both even and a multiple of 3 is 6, so the order of (12)(345) is 6. Note that the order of (12)(3456) is 4, not 8.

Having explored these examples we can easily supply the proof of the following theorem.

Theorem 1: The order of a permutation is the least common multiple of the lengths of its cycles. ☺

§2.11. Conjugates

If a, b are permutations on the same set then the **conjugate** of a by b is defined to be $b^{-1}ab$ and is denoted by $\boldsymbol{a^b}$.

Note that $b^{-1}ab = a$ if and only if $ab = ba$. So if two permutations commute, conjugating one by the other doesn't change it.

Example 9:
If a = (123)(45) and b = (16243) then
$a^b = b^{-1}ab$ = (13426).(123)(45).(16243) = (164)(35).

Notice that the permutation and its conjugate have the same cycle structure. This is in fact always the case as can be seen from the following theorem.

Theorem 2: The conjugate of $a = (x_1\ x_2\ ...\ x_n)\ ...$ by b is

$$c = a^b = (b(x_1)\ b(x_2)\ ...\ b(x_n))\ ...$$

Note: we simply replace each symbol in the cycle notation for a by its image under b.

Proof: We'll show that $ab = bc$ from which it follows that $b^{-1}ab = c$. Now

$ab(x_1) = b(a(x_1)) = b(x_2)$ and $bc(x_1) = c(b(x_1)) = b(x_2)$.

Thus ab and bc have the same effect on the symbol x_1. Similarly they have the same effect on any symbol in the cycle notation for a.

If z is any other symbol then it's fixed by a and so $ab(z) = b(a(z)) = b(z)$. Since z is not present in the cycle notation for c it's fixed by c and so

$$bc(z) = c(b(z)) = b(z).$$

We've thus shown that ab and bc behave identically on all symbols and so $ab = bc$. ☺✋

Corollary: Two permutations are conjugate if and only if they have the same cycle structure.

This theorem enables us to calculate conjugates more easily than by carrying out the two multiplications. To conjugate a by b we simply replace each symbol in the cycle notation for a by its image under b.

Example 10: If $a = (16)(275)(3948)$ and

$b = (1724)(369)$, then

$a^b = (79)(425)(6318) = (1863)(254)(79)$.

Another application of this theorem is to find conjugating permutations.

Example 11: If $a = (17)(2685)$ and $c = (1672)(35)$ find b such that $b^{-1}ab = c$.
Solution: We write the two permutations underneath one another so that the cycle lengths correspond.

$$a = (17)(2685)$$
$$c = (35)(1672)$$

We then look for a permutation that sends $1\to3$, $7\to5$, $2\to1$, $6\to6$, $8\to7$ and $5\to2$. The remaining symbols 3 and 4 are mapped to the remaining possible images 4 and 8. We could map $3\to4$ and $4\to8$ or $3\to8$ and $4\to4$. Suppose we choose the latter. Then $b = (138752)$.

There are generally several possibilities for b. Apart from the choice of images for 3 and 4 above we could have written c as (53)(6721) in which case we would want b to send $1\to5$, $7\to3$, $2\to6$ etc.

Example 12: If $a = (25)(1473)$ and $c = (46)(275)$ find b such that $b^{-1}ab = c$.
Solution: No such b exists since a and c have different cycle structures.

Because conjugates have the same cycle structure, they must have the same order. If a has order n then $b^{-1}ab$ has order n.

§2.12. Permutations in Poetry

Modern poetry, like modern music, seems to thumb its nose at rules. But in the golden age of poetry there were

complicated rhyming schemes and patterns that made writing poetry more like a piece of engineering than a creative task.

One of the most complicated poetic formats ever to be devised is the *sestina*. It seems to have originated around the twelfth century, but it's still being written.

A sestina consists basically of six stanzas, each with six lines. Instead of a rhyming scheme, each line ends in one of six words. These six words occur at the end of each line in all six stanzas, but in a different order. The order is determined by the permutation (124536). To conclude the sestina there's a short three line stanza, called the 'envoy', where the six words occur in the middle and the end of the lines in a different order again.

Rudyard Kipling, the author of the *Jungle Book*, wrote a sestina called *Sestina of the Tramp-Royal* where the lines end with the words 'all', 'world', 'good', 'long', 'done' and 'die', permuted from one stanza to the next.

Speakin' in general, I 'ave tried 'em all—
The 'appy roads that take you o'er the world.
Speakin' in general, I 'ave found them good
For such as cannot use one bed too long,
But must get 'ence, the same as I 'ave done,
An' go observin' matters till they die.

What do it matter where or 'ow we die,
So long as we've our 'ealth to watch it all —
The different ways that different things are done,

An’ men an’ women lovin’ in this world;
Takin’ our chances as they come along,
An’ when they ain’t, pretendin’ they are good?

In cash or credit—no, it aren’t no good;
You ’ave to ’ave the ’abit or you’d die,
Unless you lived your life but one day long,
Nor didn’t prophesy nor fret at all,
But drew your tucker some’ow from the world,
An’ never bothered what you might ha’ done.

But, Gawd, what things are they I ’aven’t done?
I’ve turned my ’and to most, an’ turned it good,
In various situations round the world —
For ’im that doth not work must surely die;
But that's no reason man should labour all
’Is life on one same shift — life’s none so long.

Therefore, from job to job I’ve moved along.
Pay couldn’t ’old me when my time was done,
For something in my ’ead upset it all,
Till I ’ad dropped whatever ’twas for good,
An’, out at sea, be’eld the dock-lights die,
An’ met my mate — the wind that tramps the world!

It’s like a book, I think, this bloomin’ world,
Which you can read and care for just so long,
But presently you feel that you will die

Unless you get the page you're readin' done,
An' turn another—likely not so good;
But what you're after is to turn 'em all.

Gawd bless this world! Whatever she 'ath done—
Excep' when awful long I've found it good.
So write, before I die, ''E liked it all!'

§2.13. Ringing the Changes

You've no doubt heard bells ringing out from church towers or cathedrals, even if only in films, and you probably haven't given much thought to what's going on.

You may have been vaguely aware that sometimes the bells play recognisable tunes but that more often they play abstract music.

If you hear a tune then you can be pretty sure that what you're listening to is a carillion, where the bells are controlled from a keyboard, or perhaps a recording of a carillon. If the rhythm seems regular but the notes appear random you're probably hearing English change ringing the musical equivalent of permutations. (If both the notes and the rhythm sound really random, with bells clashing

discordantly you're probably listening to continental ringing, or perhaps very bad change-ringing.)

Change ringing doesn't in fact involve random sequences, though to the untrained ear they may appear random. In the tradition of English change ringing the sequences are generated with mathematical precision.

The conventions of English change ringing (the style we hear in Australia) are a result of the way the bells are hung and the laws of physics.

You must understand that the normal rest position for bells in the English style is with the mouth uppermost. Each bell is attached to a wheel and a rope goes over the wheel and drops down to the ringing chamber below. Here you'll find, if you're able to go up into a church tower, a team of ringers standing around in a circle, pulling on the ropes. Each ringer controls just one bell, and that's a full time occupation! The upper end of the rope goes round a large wheel connected to a huge bell weighing many times more than the ringer himself.

By pulling on the rope the wheel turns and the bell rotates a full 360 degrees. During the swing the clapper strikes the bell and the note is heard. It takes about two seconds for the bell to go full circle and it's physically impossible to make the bell swing much more quickly than this without superhuman effort. And the only way to make it swing more slowly is to hold it poised, balanced in the mouth up position, and that's very difficult to do for more than a second.

This rules out tunes, unless they're played at a tenth of their normal speed because most tunes have some notes twice in quick succession. So, instead of tunes, change ringers ring permutations. Change ringing means ringing all the bells in some order followed by the same bells in a different order. Because of the physical difficulty of changing the natural time of the swing, a particular bell can't change its position in the sequence by very much each time. In fact there are normally only three possibilities. It can ring in the same position as before, or one position earlier, or one position later. This means that one or more pairs of bells swap places.

Of course this needs coordination. You can't have two bells politely saying to each other "no you go next", "no please, you go first". It all has to be tightly controlled. And this is done by the conductor who is himself one of the ringers.

It would be totally unworkable if the conductor had to schedule every single interchange, especially as they have to also control their own 'mighty beast'. So what has grown up over the centuries are 'methods'. These the ringers learn. A method takes you through maybe a dozen changes in a predetermined way. But every so often the pattern comes to a point where a call can be made. At

these points the conductor may call out “bob” or “single” which means that a different interchange is used from what would normally be the case. So the ringers follow a set pattern, appropriate to the method, but at certain stages they have to be on their toes (sometimes quite literally) ready for a ‘bob’ or a ‘single’ to be called.

A ‘bob’ and a ‘single’ are special permutations that are used to join together blocks of changes. Does the conductor call one of these whenever he or she feels like it? No it’s more complicated than that and here’s where the mathematics comes in. There’s a convention in English change ringing that **a given arrangement should never be repeated**. Not just immediately following, but n*ever* in the same piece of ringing!

There’s no aesthetic reason why a change that occurs now shouldn’t occur again in half an hour’s time. The listeners down in the street wouldn’t notice. It’s done that way because that’s the way it’s always been done. There’s a pride in getting it right.

Who keeps the score and cries foul if and when a change is repeated? Usually the pattern of bobs and singles is written out in advance. And it’s been known for a band of ringers in a bell-ringing competition to be disqualified after a couple of hours ringing because someone has proved on paper that the ‘composition’ must have repeated a change, whether or not anyone noticed at the time!

A full peal on 8 bells consists of 5040 changes and this takes over 3 hours. During this time the seven lighter

bells are rung in every one of the 7! = 5040 different arrangements with no repetitions. The heaviest bell, the tenor, stays in last place as a sort of ‘full-stop’. A quarter peal runs through exactly one quarter of this number, again with no repetitions.

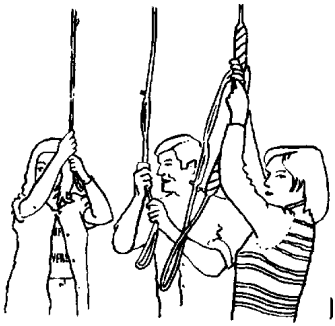
To be a really good bell-ringer you need a good knowledge of permutations. (Incidentally, if you’re dying to show off the fact that you know that the technical term for a bell ringer is ‘campanologist’ don’t! Not to a bell-ringer. Bell-ringers *never* use the term and if you use it you’ll make it clear that you’re not one of them.) Yet while you get the occasional mathematician or computer programmer in the bell-ringing fraternity, ringers are on the whole a pretty normal cross-section of the community. For centuries village churches in England have had their tower bells rung by uneducated farm labourers and shepherds who would have scratched their heads if you mentioned “1-1 and onto functions”. Their knowledge of permutations is confined to the context of their craft but within that context their knowledge may be very highly developed.

Let’s consider one of the simplest methods, Plain Bob Doubles on 6 bells, with the heaviest bell (the tenor) coming last in each change. Only the ‘front’ 5 bells are permuted so a full peal will consist of 5! = 120 changes. This will only take about 4 minutes and the method is rarely performed on so few bells.

The method consists of alternately applying the permutations $a = (12)(34)$ and $b = (23)(45)$. Ringers have

different ways of remembering what they should do but this is what it amounts to.

The ringers will begin by ringing ‘rounds’ many times. This is where the bells are rung in order 1, 2, 3, 4, 5, 6 from the highest to the lowest. The repetition at this stage doesn’t count. When the band has settled into a nice rhythm the conductor will call “go Bob Doubles”. The ringers follow the system they’ve learnt which amounts to *ababab*...



Now ab = (13542) which has order 5. So after 10 changes the bells would come back to rounds without having gone through all 120 permutations. Changing the order of the *a*’s and *b*’s wouldn’t help either because the group generated by a and b is the dihedral group of order 10. To avoid this premature repetition the conductor might insert a ‘bob’ in place of the fifth *b*. The bob for this method is c = (34). This causes the ringing to go off on another track of a new 10 changes.

So if a bob is called at the end of each set of 10 changes the pattern will correspond to the sequence $(ab)^4ac(ab)^4ac$...

But $(ab)^4ac$ = (12453)(12) = (2453) so after 4 lots of this pattern of 10 changes we’d come back to rounds prematurely. So before this happens the conductor will call ‘single’, which is a different permutation again.

Bell-ringing is in no danger of dying out as in the last seventy or eighty years there has been a resurgence of interest in bell ringing around the world, and especially in Australia. There are now 64 towers in Australia capable of English bell ringing, 50 in the USA, 7 in NZ and many hundreds in the UK.

They're generally willing to show visitors how it's done. Contact the church or, if the door is open at the bottom of the tower when they're ringing, go on up. But if all the ringers are occupied ringing, don't even *think* of interrupting them! And don't expect to be able to have a go yourself. It's quite difficult and even dangerous for an untrained person to just ring a single note. If you don't apply the correct tension the rope could fly about all over the place. Even if you're willing to 'learn the ropes' it would be several months before you'd be allowed to do it on your own.

§2.14. Disorder and Sorting

An **inversion** of a permutation π on the set $[n]$ is a pair of numbers whose order is reversed by π, that is pairs (i, j) where $i < j$ but $\pi(i) > \pi(j)$.

The **disorder** of a permutation π on $[n]$ is $\mathbf{\Delta(\pi)}$ = the number of its inversions. It's a measure of how mixed up the arrangement 1 2 3 ... n becomes after the permutation has been applied. The disorder of the identity permutation is 0.

If the sequence is totally reversed and becomes

$$n, n-1, \ldots, 2, 1,$$

the disorder is ½ $n(n-1)$ since every one of the pairs is out of order. For all $\pi \in \mathbf{S}_n$, $0 \le \Delta(\pi) \le \frac{1}{2} n(n-1)$.

Example 13: Let $\pi = (135)(24)$. This changes 12345 into 54123. (What was previously in position 5 is now in position 1, etc.) There are 7 inversions: (1,4), (1,5), (2,4), (2,5), (3,4), (3,5), (4,5) so $\Delta(\pi) = 7$. For example, (1,5) is an inversion because 1 comes before 5 in 12345 but 5 comes before 1 in 54123.

Apart from the identity, the permutations with the smallest disorder are those which swap two adjacent symbols and fix all the rest. These have disorder 1 and are transpositions of the form $s_i = (i \quad i+1)$. They're called **simple transpositions**.

Theorem 3: For all permutations π and all simple transpositions s_i, $\Delta(\pi\,(s_i)) = \Delta(\pi) \pm 1$
Proof: Suppose $\pi(a) = i$ and $\pi(b) = i + 1$.
If $a < b$ then (a, b) is an inversion for $\Delta(\pi\,(s_i))$ but not for π and hence $\Delta(\pi\,(s_i)) = \Delta(\pi) + 1$.
Similarly if $a > b$ $\Delta(\pi\,(s_i)) = \Delta(\pi) - 1$. ☺✌

There are many algorithms for sorting arrays of data on a computer. One of the simplest is known as Bubble Sort. It's not the most efficient of the sorting algorithms, though it's not too bad. What it has going for it is that it's extremely simple to describe and, more

importantly for us, it gives us an important theoretical result.

The name Bubble Sort arises from the fact that 'lighter' elements (those that come earlier in the ordering), bubble up to the top as we continue to swap a number with the one immediately above it until they all reach their proper position.

BUBBLE SORT

To sort a set:

(1) FOR all $i < n$, IF the i'th and $(i+1)$'st are out of order THEN swap them.

(2) IF a swap was made, GOTO (1) and do it again. Otherwise END.

Example 14: BUBBLE SORT on 34521:
34**52**1→342**51**→3**42**15→32**41**5→**32**145→2**31**45
→**21**345→12345 (7 swaps).

Theorem 4: A permutation π is the product of $\Delta(\pi)$ simple transpositions and no fewer.

Proof: Each swap in Bubble Sort reduces the disorder by 1. ☺✋

The following table gives the disorder of all the elements of $\mathbf{S}_4$. Note that exactly half have even disorder while the rest have odd disorder.

EVEN DISORDER	
π	$\Delta(\pi)$
I	0
(123)	2
(132)	2
(124)	4
(142)	4
(134)	4
(143)	4
(234)	2
(243)	2
(12)(34)	2
(13)(24)	4
(14)(23)	6

ODD DISORDER	
π	$\Delta(\pi)$
(12)	1
(13)	3
(14)	5
(23)	1
(24)	3
(34)	1
(1234)	3
(1243)	3
(1324)	5
(1342)	3
(1423)	5
(1432)	3

§2.15. Odd and Even Permutations

The **parity** of a permutation π is:

$$\mathbf{P(\pi)} = \Delta(\pi) \pmod 2.$$

If $P(\pi) = 0$ we say that π is an **even** permutation.
If $P(\pi) = 1$ we call π an **odd** permutation.

Theorem 5: $P(ab) = P(a) + P(b) \pmod 2$.

Proof: Let $b = t_1 \ldots t_k$ be a factorisation into $k = \Delta(b)$ simple transpositions. (See Theorem 4.)

Then $\Delta(at_i) = \Delta(a) \pm 1$ and so

$$P(at_i) = P(a) + 1 \text{ (modulo 2).}$$

Hence $P(ab) = P(a) + k \pmod 2$

$= P(a) + P(b)$. ☺✋

Corollary: Inverses have the same parity as each other.
Proof: $aa^{-1} = 1$ so if a and a^{-1} had opposite parity then I would have odd parity.

This theorem shows that odd-ness and even-ness of permutations behave under multiplication like odd and even numbers under *addition*. That is:

even × even = even
even × odd = odd
odd × even = odd
odd × odd = even

The fact that even × even is even, the inverse of an even permutation is even and the identity permutation is even means that the set of even permutations is a group under permutation multiplication. We call this group the **alternating group of degree *n*** and denote it by $\mathbf{A}_n$. It is a **subgroup** of $\mathbf{S}_n$. Note that $\mathbf{A}_1 = \{I\} = \mathbf{S}_1$.

Example 15:
$\mathbf{A}_4$ = {I, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)}

Theorem 6: Conjugates have the same parity as each other.
Proof: $P(g^{-1}hg) = P(g) + P(h) + P(g) = P(h) \pmod 2$.

Corollary: Transpositions are odd.
Proof:
They're conjugate to the simple transposition (12). ☺✋

Theorem 7: A cycle of length n is a product of $n - 1$ transpositions.
Proof: $(x_1\ x_2\ \ldots\ x_n) = (x_1\ x_2)(x_1\ x_3)\ \ldots\ (x_1\ x_n)$.
Corollary: Cycles of odd length are even and cycles of even length are odd. ☺✋

Example 16: (123456) is odd since its length is even; (123)(45)(6789) is even [even × odd × odd]

Theorem 8: If $n > 1$ exactly half the permutations in $\mathbf{S}_n$ are even.
Proof: The map $\pi \rightarrow \pi(12)$ is a 1-1 correspondence between the even and odd permutations so there's the same number of each. ☺✋
Corollary: If $n > 1$, the order of $\mathbf{A}_n$ is $\frac{1}{2}\, n!$

§2.16. Permutation Puzzles

The Rubik's™ Cube, one of the most famous puzzles of all time, is just one of a class of puzzles that involve permutations. The common feature is that there are several pieces to be rearranged in a certain pattern by a sequence of basic moves. In many of these puzzles the engineering dictates what's possible while in others the limitations are imposed by rules.

As a very simple puzzle consider the following. Arrange 5 coins, one each of 5¢, 10¢, 20¢, $1 and $2, in a row in ascending order of value from left to right. The allowable moves are:

(1) swap the coins at each end;

(2) move the left-most coin to the right hand end.

The goal is to reverse the order of the coins.

This puzzle is not hard to solve without mathematics but let's analyse it using permutations. We can label the five coins 1, 2, 3, 4, 5 and the problem is to go from the arrangement 12345 to 54321. The permutation that does this is $g = (15)(24)$. This is our **goal permutation**. The allowable moves can also be expressed as permutations. Swapping the two ends is $a = (15)$ while moving the left-hand coin to the right is $b = (15432)$. The puzzle is solved once you have expressed g in terms of a and b.

Now as can be verified, $ab^2abab^4ab^3 = (15)(24) = g$. Never mind for now how we might find such a sequence. The fact is that it's a sequence of a's and b's that achieves the goal. So if the coins are arranged in the order 12345 and we carry out the basic moves according to the recipe $abbababbbbabbb$ we obtain the required reversal. Use 5 coins, or five small scraps of paper, to verify that this is indeed so.

Now I'm not claiming that this represents the *shortest* solution. Perhaps you can find a shorter one by trial and error. But at least this solution can be found by a

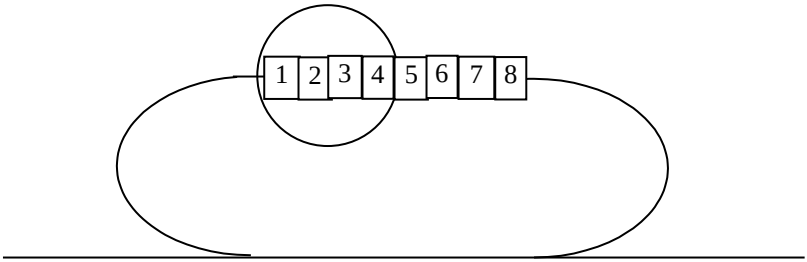
systematic procedure that I'll explain now in the context of another puzzle.

§2.17. The Shunting Puzzle

In a certain shunting yard there's a loop of track. On one side of the loop there's a turntable. This turntable can only operate with four carriages. It isn't big enough to accommodate more than four and for some mysterious reason (imposed to keep the puzzle from becoming trivial) it will not operate with fewer than four carriages.

On this loop of track there's a train consisting of an engine followed by six carriages and a guard's van at the end. The engine and guard's van each count as a carriage for the purpose of the turntable rule.

The problem is to interchange the engine and the guard's van while keeping the six carriages between them in the same order. This must be done only using the loop of track and the turntable. Any number of carriages can be taken around the loop at any time and the turntable can be operated at any time so long as it has exactly four pieces of rolling stock on it.



This may not sound like a problem that's likely to arise in real life but there are some situations which require a similar analysis but which are rather more complicated to describe. You can simulate this puzzle by sticking little labels on eight coins. The turntable can be simulated by putting four fingers on four adjacent coins and rotating. You may wish to attempt to solve the puzzle before proceeding with the mathematical analysis.

For convenience I use the symbols 2, 3, 4, 5, 6, 7 to represent the six carriages with 1 representing the engine and 8 the guard's van. The initial arrangement is 12345678 and the arrangement we have to achieve is 82345671. The goal permutation is thus G = (18).

Now there are two basic operations at our disposal. We can take one carriage from the left-hand side of the train around the loop to the right-hand side. (We shall consider the engine and guard's van as carriages).

This operation corresponds to the permutation L = (18765432) since the carriage that was previously in position 1 ends up in position 8 and so on. Everything that can be achieved with just the loop can be expressed in terms of L. For example, taking a number of carriages around at the same time is equivalent to taking them one by one and so is expressible as a power of L. Taking a carriage from the right-hand end around to the left is just L^{-1}.

The turntable gives an additional basic move. Let T = (14)(23). Don't forget that these symbols here refer to the positions, not the numbers of the carriages that

occupy them, and we can agree to number the positions starting with the four on the turntable. Removing the mathematically irrelevant setting of the puzzle we can express it very simply as:

Generate G = (18) in terms of
L = (18765432) and T = (14)(23).

Our goal is to generate a particular 2-cycle. But let's start by trying to generate *any* 2-cycle.

Begin by randomly multiplying L's and T's together in a trial-and-error fashion. The product TL = (13)(48765). Now this isn't our goal, nor is it even a 2-cycle. But notice that because it's a transposition times a 5-cycle, we can remove the 5-cycle by raising TL to the fifth power: $(TL)^5 = (13)$.

Of course we were lucky to hit upon a permutation of the right shape so quickly. There's a certain amount of trial-and-error in the method. But its advantage over completely mindless trial-and-error is that we widen our goal from a specific permutation to a whole class of permutations.

We still have to get from this 2-cycle (13) to (18), the one we want. We do this by conjugation. Remember that conjugation preserves the cycle structure. So conjugating $(TL)^5$ by any permutation gives a 2-cycle. Of course the conjugating permutation would need to be expressible in terms of T and L.

So we need to find a permutation, expressible in terms of T and L, that takes 1 to 1 and 3 to 8. (Or we could instead find one that takes 1 to 8 and 3 to 1.)

We'll keep to the first case. We need a permutation that fixes 1. Neither T nor L by themselves fix 1. But notice that T takes 1 to 4 and L^3 takes 4 back to 1 so TL^3 = (285)(3746) fixes 1. But it doesn't send 3 to 8. Not even some power of it sends 3 to 8 because 3 and 8 are in different cycles. Never mind, we might find another possibility.

Notice that $(TL)^2$ fixes 1. In fact $(TL)^2$ = (47586). Does this send 3 to 8? No, 3 and 8 are again in different cycles. Remember 3 is fixed so it is in a cycle by itself.

So neither TL^3 = (285)(3746) nor $(TL)^2$ = (47586) separately do what we want – but together they can. $(TL^3)^{-1}$ sends 3 to 6 and $(TL)^{-2}$ sends 6 to 8. So we get from 3 to 8 by 'changing trains' at 6.

The product of these permutations is $(TL^3)^{-1}(TL)^{-2}$ = (2738). This fixes 1 and sends 3 to 8 and most importantly, it's generated by T and L. We simply conjugate $(TL)^5$ by $(TL^3)^{-1}(TL)^{-2}$ and this will produce a T-L expression for our goal.

So (18) = $[(TL^3)^{-1}(TL)^{-2}]^{-1}\ (TL)^5\ [(TL^3)^{-1}(TL)^{-2}]$

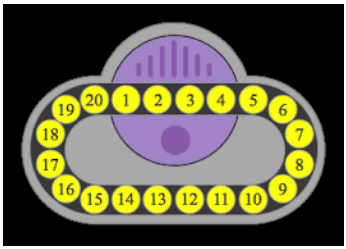
= $(TL)^2(TL^3)\ (TL)^5(TL^3)^{-1}(TL)^{-2}$

= $(TL)^2(TL^3)\ (TL)^5L^{-3}T^{-1}L^{-1}T^{-1}\ L^{-1}T^{-1}$

= $(TL)^2(TL^3)\ (TL)^5L^5TL^7T\ L^7T$

= $TLTLTL^3TLTLTLTLTLL^5TL^7TL^7T$.

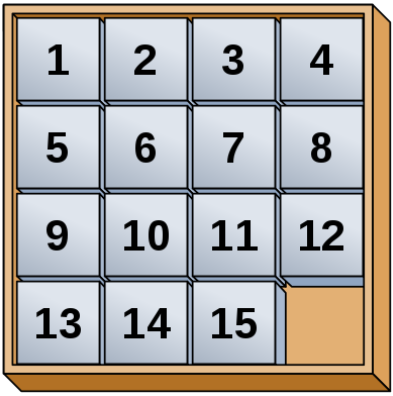
Convince yourself that it works by labelling eight coins and carefully performing this recipe. As I said before it may not be the shortest solution, but it is a solution. And although it involved a certain amount of trial-and-error it was intelligent trial-and error!



I have been using this example for several decades in my online notes and I like to think that the following manufactured puzzle was inspired by mine. This one has 20 ‘carriages’. The turntable rule is dictated by the design rather than simply as an arbitrary rule, because there is only just enough space around the loop to accommodate the 20 discs and so it’s only possible to operate the turntable if it contains 4 discs.

§2.18. The 15-Puzzle

Another example of a puzzle where the basic moves are dictated by the mechanism is the so-called 15-puzzle. I can’t take credit for this one because I remember it as a schoolboy in the 1950s! A square tray contains 15 small tiles, numbered from 1 to 15, arranged in a 4×4 array with one spot empty. The tiles can



slide horizontally or vertically into the empty position. The goal is to get a particular pattern.

Because the pieces are slotted into each other they can't be removed from the frame so the only allowable moves are those that are physically possible by sliding the tiles into the empty place. What are they?

Clearly there are four basic moves L, R, U and D where:

L = move a tile left into the empty space,
R = right,
U = up and
D = down.

Various patterns were set as goals. For example if the square is in some random starting configuration the goal might be to obtain the numbers in order as in the illustration. Of course the solution will depend on the starting pattern, but it should be possible to express the recipe as a long sequence of L's R's U's and D's.

What are these moves as permutations? Sliding a tile in effect swaps that tile and the empty space next to it and this suggests we should be treating it as a transposition (××). The trouble is that we have to permute positions, not tiles, and so we can't treat the empty space as a dummy tile. The transposition (12) can't be achieved if both positions are currently occupied – only if one of them is empty. Obviously this sort of conditionality is unworkable.

The way around this dilemma is to have the empty space return to the bottom-right corner from time to time and to record the permutation only at these stages. We are therefore considering permutations on the remaining 15 positions.

So while we can't consider L by itself as such a permutation, the sequence RDLU can be. It rotates the three tiles surrounding the bottom-right corner and gives the permutation A = (11 15 12). Now it's clear that essentially the only basic moves that are possible are to rotate the tiles around a rectangle that has the blank in the bottom-right corner. These will be cycles of odd length and so will be even permutations. So only even permutations are possible. Engraved on the back of these little plastic puzzles were some patterns to achieve. But there was one pattern marked IMPOSSIBLE. The reason why it was impossible is that it would require an odd permutation. Of course we boys soon discovered how to snap the tiles out of the frame using a pen knife and reassemble them to the impossible pattern!

I remember that the first Rubiks cubes has stick-on labels for the colours and my young son 'solved' the puzzle very quickly. Unfortunately he wasn't all that neat in sticking the labels back on and so it was pretty obvious how he had solved it.

The key to solving most permutation puzzles is to generate permutations that end up fixing most of the tiles. A very useful way of doing this to use **commutators**.

These are expressions of the form $X^{-1}Y^{-1}XY$. The name reflects the fact that X and Y commute if and only if their commutator is the identity.

With the 15-puzzle, rotating the tiles around the bottom right-hand 2×2 square gives the permutation A = RDLU = (11 15 12). Although R, D, L and U are not permutations as such note that this is the commutator $L^{-1}U^{-1}LU$. Another useful rotates the tiles anticlockwise around the bottom two rows. It is $B = (LLL)^{-1}U^{-1}(LLL)U$. = (9 13 14 15 12 11 10). This may not seem very useful permutation, but wait. If we calculate $C = A^{-1}B^{-1}AB$ we get C = (10 15)(11 12).

So we somehow get the right tiles to occupy positions 11 and 12. Then, if we conjugate C by permutations that fix 11 and 12 we can easily rearrange the other tiles. The tiles in positions 11 and 12 will just swap back and forth. If the pattern is possible the tiles in those positions will automatically be the right way round. If every other tile is in the right place but those in positions 11 and 12 are the wrong way round this will mean that the pattern is impossible.

EXERCISES FOR CHAPTER 2

Exercise 1: Write the following permutations in cycle notation:

(a) $1\to3$, $2\to4$, $3\to5$, $4\to1$, $5\to2$;
(b) $1\to4$, $2\to5$, $3\to3$, $4\to2$, $5\to1$;
(c) $1\to2$, $2\to4$, $3\to5$, $4\to1$, $5\to3$;
(d) $1\to1$, $2\to5$, $3\to3$, $4\to4$, $5\to2$;
(e) $1\to1$, $2\to2$, $3\to3$, $4\to4$, $5\to5$;
(f) $1\to2$, $2\to1$, $3\to3$, $4\to5$, $5\to4$.

Exercise 2: Which of the following is not a permutation?

(a) $1\to3$, $2\to4$, $3\to2$, $4\to1$;
(b) $1\to1$, $2\to4$, $3\to3$, $4\to1$;
(c) $1\to3$, $2\to2$, $3\to1$, $4\to4$.

Exercise 3: Which of the following permutations is different to the other two.

(a) (1428)(375);
(b) (1824)(573);
(c) (753)(2814).

Exercise 4: Write down all of the permutations in $\mathbf{S}_5$ with each of the following cycle structures:
(a) $(\times\times)$; (b) $(\times\times\times\times)$; (c) $(\times\times)(\times\times)$;

Exercise 5: Write down all of the cycle structures in S_6 together with the number of each.

[Do not list the permutations themselves. There are too many!]

Exercise 6: Perform the following permutation multiplications:
(a) (132) × (13); (b) (1423) × (1342);
(c) (12)(34) × (123); (d) I × (1253); (e) (12) × (34).

Exercise 7: Find the inverse of the following permutations:
(a) (154)(263); (b) (17246)(35);
(c) I; (d) (12)(34)(56); (e) (15)(2354).

Exercise 8: If a = (253)(46) and b = (126) calculate the following:
(a) ab; (b) $(ab)^{-1}$;
(c) a^{-1}; (d) b^{-1};
(e) $a^{-1}b^{-1}$; (f) $b^{-1}a^{-1}$.

Exercise 9: Write down the orders of the following permutations:
(a) (12345); (b) (12345)(78);
(c) (123456)(78); (d) (12)(34)(56)(78); (e) I;
(f) (15)(2354).

Exercise 10: In each of the following cases find the order of ab:

(a) $a = (123)$, $b = (12)$;
(b) $a = (123)$, $b = (45)$;
(c) $a = (123)$, $b = (14)$;
(d) $a = (123)$, $b = (12)(34)$;
(e) $a = (123)(456)$, $b = (34)(56)$;
(f) $a = (123)(456)(789)$, $b = (34)(67)$.

[Note that in all cases, a has order 3 and b has order 2 yet the order of ab is different in all five cases. This shows that there is no connection between the order of a product and the orders of its factors – unless the factors involve disjoint cycles.]

Exercise 11: Prove that there is no upper bound to the order of the product of a permutation of order 3 with a permutation of order 2.

Exercise 12: Find the largest order for any of the elements of $\mathbf{S}_{10}$.

Exercise 13: If $a = (1234)(567)$ find the order of each of the following:
(a) a^{-1}; (b) a^2; (c) a^3; (d) a^4; (e) a^5.

Exercise 14: Find $a^b = b^{-1}ab$ in each of the following cases (use the shortcut to conjugate):

(a) $a = (12)$, $b = (2345)$;
(b) $a = (13)(256)$, $b = (23)(45)$;

(c) $a = (14)(25)$, $b = (1325)$;
(d) $a = (1325)$, $b = (14)(25)$;
(e) $a = (156)$, $b = (156)$.

Exercise 15: Where possible find a permutation $b \in \mathbf{S}_6$ such that $a^b = c$ in each of the following cases:
(a) $a = (132)(45)$, $c = (15)(234)$;
(b) $a = (14)(23)$, $c = (16)(24)(35)$;
(c) $a = (12)(34)$, $c = (13)(24)$;
(d) $a = (14)$, $c = \mathrm{I}$;
(e) $a = (13)$, $c = (13)$.

Exercise 16: Express each of the following permutations as a product of transpositions (cycles of length 2): (a) (15624); (b) (2546)(357); (c) I.

Exercise 17: Which of the following are even permutations? (a) (123456789); (b) (123456)(789); (c) (123)(4567)(89); (d) (12)(345)(67)(89); (e) (123)(456)(789).

Exercise 18: Express $g = (123)(456)$ in terms of $a = (12)$ and $b = (23456)$.

Exercise 19: Express $g = (259)(37)$ in terms of $a = (12)$ and $c = (123456789)$.

Exercise 20:

(i) If a = (142357) and b = (25) (47) find ab, a^2, and $b^{-1}ab$.

Prove that the group generated by a, b is the dihedral group of order 12.

(ii) If $\langle a \rangle$ denotes the set of powers of a (this is called the cyclic subgroup generated by a), find the elements of $\langle a \rangle$.

(iii) If a = (123) (56) find the elements of $\langle a \rangle \cap \mathbf{A}_6$.

(iv) If a = (14) (253) and b = (123) (45) then find all the even permutation $x \in \mathbf{A}_5$ such that

$$a = x^{-1}bx.$$

(v) If a = (12453), b = (23) and c = (123) then express c in terms of a, b.

[**HINT:** Write c = (231) = (23)(21) = (23)(12).]

Prove that neither a nor b can be expressed in terms of the other two.

Exercise 21: Where possible, solve the following modified versions of the shunting puzzle. In each case the term 'carriage' includes the engine and guard's van:

(a) 6 carriages, 4 on the turntable;

(b) 5 carriages, 4 on the turntable;

(c) 7 carriages, 3 on the turntable.

(d) 8 carriages, 3 on the turntable.

[**HINT**: for (d): consider the algebraic expression $E = x_1 x_3 x_5 x_7 + x_2 x_4 x_6 x_8$.]

Exercise 22: Take eight coins and label them the letters DEARGRAN. Starting with the coins in this order and using the two basic operations of the shunting yard problem, obtain the arrangement ARRANGED.

Exercise 23: Solve the following permutation puzzle:

7	6	5
	hole	4
1	2	3

Start with seven coins and a grid of nine squares as indicated in the following diagram:

Seven of the eight outside squares are each occupied by a coin and the middle square represents a hole. The coins may move around the edge of the hole, or a coin may 'jump over the hole'. Jumping over the hole must be done in a straight line only, either vertically or horizontally into the empty square. The object of the puzzle is to produce the arrangement:

1	2	3
	hole	4
7	6	5

SOLUTIONS FOR CHAPTER 2

Exercise 1: (a) (13524); (b) (1425); (c) (124)(35); (d) (25); (e) I; (e) (12)(45).

Exercise 2: (b) is not because both 1 and 4 map to 1 (not 1-1) and nothing maps to 2 (it is not onto).

Exercise 3: (a) = (c) (they only look different because the cycles start in different places) but (b) is different since under (b) $1 \to 8$ while under (a) and (c) $1 \to 4$. In fact (b) is the inverse of the other two.

Exercise 4:

(a) (12), (13), (14), (15), (23), (24), (25), (34), (35), (45);

(b) (1234), (1235), (1243), (1245), (1253), (1254), (1324), (1325), (1342), (1345), (1324), (1325), (1423), (1425), (1432), (1425), (1432), (1435), (1523), (1524), (1532), (1534), (1542), (1543), (2345), (2354), (2435), (2453), (2534), (2543);

(c) (12)(34), (12)(35), (12)(45), (13)(24), (13)(25), (13)(45), (14)(23), (14)(25), (14)(35), (15)(23), (15)(24), (15)(34), (23)(45), (24)(35), (25)(34).

Note carefully that these elements have been listed in a systematic order. This makes it much easier to ensure that there are no duplicates, and more importantly, that nothing has been left out. In each position we write down the smallest possibility that remains. You should also

count the number of permutations of each type and see if you could have predicted that from the systematic ordering.

Exercise 5:

Cycle structure (××): There are 6 possibilities for the first position and 5 remaining ones for the 2nd position, giving $6 \times 5 = 30$ possibilities. But each will have been counted twice since $(xy) = (yx)$. So there are 15 permutations with this cycle structure.

Cycle structure (×××): There are $6 \times 5 \times 4$ possible ways of filling up the places but each occurs 3 times so the number of permutations is $\frac{6 \times 5 \times 4}{3} = 40$.

Cycle structure (××)(×××): There are $\frac{6 \times 5 \times 4 \times 3 \times 2}{2 \times 3}$ = 120 permutations with this structure. We divide by 2 for the 2-cycle and by 3 for the 3-cycle.

Cycle structure (××)(××): There are $\frac{6 \times 5 \times 4 \times 3}{2 \times 2 \times 2} = 45$ permutations of this type. We divide by 2 for each cycle and we need to divide by 2 a third time to allow for the fact that we'll have still counted each permutation twice by virtue of the fact that (ab)(cd) = (cd)(ab).

Cycle structure (××)(××)(××): There are $\frac{6 \times 5 \times 4 \times 3 \times 2 \times 1}{2 \times 2 \times 2 \times 6} = 15$ of these. As well as dividing

by 2 for each of the 2-cycles we need to divide by 3! = 6 to take account of the fact that the three 2-cycles can be permuted in any order without changing the permutation. The following table gives all possible cycle structures and the number of permutations of each type.

cycle structure	**calculation**	**number**
I	1	1
$(\times\times)$	$\frac{6\times5}{2}$	15
$(\times\times\times)$	$\frac{6\times5\times4}{3}$	40
$(\times\times\times\times)$	$\frac{6\times5\times4\times3}{4}$	90
$(\times\times\times\times\times)$	$\frac{6\times5\times4\times3\times2}{5}$	144
$(\times\times\times\times\times\times)$	$\frac{6\times5\times4\times3\times2\times1}{6}$	120
$(\times\times\times\times)(\times\times)$	$\frac{6\times5\times4\times3\times2}{4\times2}$	90
$(\times\times\times)(\times\times\times)$	$\frac{6\times5\times4\times3\times2\times1}{3\times3\times2}$	40
$(\times\times\times)(\times\times)$	$\frac{6\times5\times4\times3\times2}{3\times2}$	120
$(\times\times)(\times\times)$	$\frac{6\times5\times4\times3}{2\times2\times2}$	45
$(\times\times)(\times\times)(\times\times)$	$\frac{6\times5\times4\times3\times2\times1}{2\times2\times2\times6}$	15
TOTAL		**720**

Exercise 6: (a) (23); (b) (124); (c) (134); (1253); (e) (12)(34).

Exercise 7: (a) (145)(236); (b) (16427)(35); (c) I; (d) (12)(34)(56); (e) (15324). This is a trick question since (15)(2354) is not cycle notation for a single permutation because the cycles aren't disjoint. Rather it's the product of two permutations and must first be simplified. (15)(2354) = (14235) so the inverse is (15324).

Exercise 8: (a) (125364); (b) (146352); (c) (235)(46); (d) (162); (e) (164235);
(f) (146352). Note that $(ab)^{-1} = b^{-1}a^{-1}$. This is always the case.

Exercise 9: (a) 5; (b) 10; (c) 6; (d) 2; (e) 1; (f) 5. This is a trick question because the cycles aren't disjoint. When simplified this permutation becomes (14235).

Exercise 10: (a) 2; (b) 6; (c) 4; (d) 3; (e) 5; (f) 9

Exercise 11: $(123)(456)\ \ldots\ (3n{-}2\ 3n{-}1\ 3n) \times (34)(67)(9\ 10)\ \ldots\ (3n{-}3\ 3n{-}2)$
$= (1\ 2\ 4\ 5\ 7\ \ldots\ 3n{-}2\ 3n{-}1\ 3n\ 3n{-}3\ 3n{-}6\ \ldots\ 3)$ which has order $3n$.

Exercise 12: 30. [Consider the cycle structure (××)(×××)(×××××).]

Exercise 13: (a) 12; (b) 6; (c) 4; (d) 3; (e) 12.

Exercise 14: (a) (13); (b) (12)(346);
(c) (34)(51) = (15)(34); (d) (4352) = (2435);
(e) (156).

Exercise 15: (a) (124); (b) none; (c) (23); (d) none; (e) I. (Other answers are possible.)

Exercise 16: (a) (15)(16)(12)(14);
(b) (25)(24)(26)(35)(37); (c) (12)(12) (in fact I can be considered as a product of zero transpositions).

Exercise 17: (a), (c), (e) are even. The others are odd.

Exercise 18: g = (12)(13)(45)(46).
Now (12) = a, (13) = a^b, (45) = (14)(15)(14)
= $a^{b^2}a^{b^3}a^{b^2}$, (46) = (14)(16)(14) = $a^{b^2}a^{b^4}a^{b^2}$ so
$g = a\ b^{-1}ab\ b^{-2}ab^2\ b^{-3}ab^3\ b^{-2}ab^2\ b^{-2}ab^2\ b^{-4}ab^4\ b^{-2}ab^2$
$= ab^{-1}ab^{-1}ab^{-1}ab^{-3}ab^2ab^2$

Exercise 19: g = (25)(29)(37).
Let $d = ca$ = (23456789). Then (13) = a^d, (14) = a^{d^2}, etc
Now (25) = (12)(15)(12) = $a\ a^{d^3}\ a$,
(29) = (12)(19)(12) = $a\ a^{d^{-1}}\ a$,
(37) = (13)(17)(13)
= $a^d\ a^{d^{-3}}\ a^d$.
So $g = ad^{-3}ad^3a\ adad^{-1}a\ d^{-1}add^3ad^{-3}d^{-1}ad$

$= ad^{-3}ad^3a^2dad^{-1}ad^{-1}ad^4ad^{-4}ad$

$= a(ca)^{-3}a(ca)^3a^2ca^2(ca)^{-1}a(ca)^{-1}a(ca)^4a(ca)^{-4}aca$

$= aa^{-1}c^{-1}a^{-1}c^{-1}a^{-1}c^{-1}acacaca\ a^2ca^2a^{-1}c^{-1}acacacaca$
$aa^{-1}c^{-1}a^{-1}c^{-1}a^{-1}c^{-1}a^{-1}c^{-1}\ aca$

$= c^{-1}a^{-1}c^{-1}a^{-1}c^{-1}acacaca^3cac^{-1}acacacacac^{-1}a^{-1}c^{-1}$
$a^{-1}c^{-1}a^{-1}c^{-1}aca$

$= c^{-1}ac^{-1}ac^{-1}acacaca^3cac^{-1}acacacacac^{-1}ac^{-1}ac^{-1}$
$ac^{-1}aca$ since $a^2 = I$.

Exercise 20:

(i) ab = (17)(23)(45), a^2 = (125)(374), $b^{-1}ab$ = (175324) = a^{-1} so the group generated by a, b is the dihedral group of order 12 (note that a has order 6 and b has order 2).

(ii) $\langle a \rangle$ = {I, (142357), (125)(374), (13)(27)(45), (152)(347), (175324)}.

(iii) The element a is itself odd, and so all its odd powers will also be odd. However its even powers, 1, a^2 and a^4 will all be even, so $\langle a \rangle \cap \mathbf{A}_6 = \{I, a^2, a^4\}$.

(iv) Writing a = (14)(253) and b = (45)(123) we might consider the permutation (1452). This conjugates b into a but it is odd, not even. There are altogether 6 ways of writing b:

b = (45)(123) = (45)(231) = (45)(312) = (54)(123)
= (54)(231) = (54)(312) giving rise to just the following possibilities for x:

(1452), (1453), (145)(23), (152), (153), (15)(23).

Just the last 3 of these are even, so there are three possibilities for x: (152), (153), (15)(23).

(v) c = (23)(12). We have to now express (12) in terms of a, b. We'll conjugate b by something suitable to get (21). Such a permutation would fix 2 and send 3 to 1. But, of course, it must be expressible in terms of a, b. Now ab = (13)(245) so $(ab)^3$ = (13) does exactly what we want. This means that $(ab)^{-3}b(ab)^3$ = (12) and so $c = b(ab)^{-3}b(ab)^3$.

Why can't a be expressed in terms of b, c? Simply because both b, c fix 4 and 5 and so any combination of them would have to do likewise. But a doesn't fix them.

And why can't b be expressed in terms of a and c? The answer in this case is that both a and c are even permutations, and so anything built up from them would also have to be even, while b is odd.

Exercise 21:

(a) a = (123456), b = (14)(23). Goal = (16).
Now ab = (13)(456) so $(ab)^3$ = (13).
We want to conjugate this to (16) and so we want a permutation that fixes 1 and sends 3 to 6. Now a^3 maps 1 to 4 and 4 maps 4 back to 1 so a^3b = (2536) fixes 1. Well, what do you know? It also sends 3 to 6.
So $(a^3b)^{-1}(ab)^3a^3b$ = (16).

(b) a = (12345), b = (14)(23). Goal = (15).
This is impossible since both a, b are even.

(c) a = (1234567), b = (13). Goal = (17). We want to conjugate (13) to (17) and so we want a permutation that fixes 1 and sends 3 to 7. Now ab = (12)(34567) and so $(ab)^2$ = (35746) fixes 1. It doesn't map 3 to 7, but its square does. So $(ab)^{-4}b(ab)^4$ = (17).

(d) This is impossible, though the reason has nothing to do with odd and even permutations.
Consider the algebraic expression E = $x_1\,x_3\,x_5\,x_7 + x_2\,x_4\,x_6\,x_8$. Both permutations a, b leave the value of E unchanged and therefore it will be unchanged by anything generated by them. But the goal permutation, applied to the subscripts of E, would change it into
$x_8\,x_3\,x_5\,x_7 + x_2\,x_4\,x_6\,x_1$ which certainly is different to E.

Exercise 22:
For convenience put 1 = D, 2 = E, 3 = A, 4 = R, 5 = G, 6 = R, 7 = A, 8 = N. Our goal permutation is g = (185627)(34), although (185427)(36) would do just as well because of the two R's. We have to express this in terms of a = (12345678) and b = (14)(23).
Now ab = (13)(45678) so $(ab)^5$ = (13). We can conjugate this to produce other 2-cycles.
Our goal permutation can be expressed as g = (18)(15)(16)(12)(17)(34). Even this last can be expressed in a similar form by writing (34) = (13)(14)(13), so

g = (18)(15)(16)(12)(17)(13)(14)(13).

Of course, (13) is just b. We want permutations that fix 1. Now $(ab)^2$ = (46857) is one such, but it doesn't map

3 to anything other than itself. Note that under a^3, $1 \to 4$ and b sends this back to 4. Hence a^3b = (258)(3647) fixes 1 and is a little more useful when it comes to 3. It maps 3 to 6, its inverse maps 3 to 7 and its square maps 3 to 4.

Hence (16) = $(a^3b)^{-1}(ab)^5a^3b$, (17) = $a^3b\ (ab)^5\ (a^3b)^{-1}$ and (14) = $(a^3b)^{-2}(ab)^5(a^3b)^2$.

For (18), (15) and (12) we need to use a combination of a^3b and $(ab)^2$.

Now a^3b sends 3 to 6 and $(ab)^2$ sends 6 to 8 (both fix 1) so $a^3b(ab)^2$ conjugates (13) to (18).

Hence (18) = $(a^3b(ab)^2)^{-1}\ (ab)^5\ a^3b(ab)^2$.

Similarly a^3b sends 3 to 6 and $(ab)^4$ sends 6 to 5 so $a^3b(ab)^4$ conjugates (13) to (15).

Hence (15) = $(a^3b(ab)^4)^{-1}\ (ab)^5\ a^3b(ab)^4$.

The cycle (12) is a little more difficult, but we can use $(ab)^2$ and a^3b to get 3 to 2. We first map 3 to 6 by a^3b then go from 6 to 8 by $(ab)^2$ and finally use a^3b again to move 8 to 2. Hence (12) = $[a^3b(ab)^2a^3b]^{-1}(ab)^5\ [a^3b(ab)^2a^3b]$.

Putting this all together we get:

g = $[(a^3b(ab)^2)^{-1}\ (ab)^5a^3b(ab)^2]\ [(a^3b(ab)^4)^{-1}(ab)^5\ a^3b(ab)^4]\ [(a^3b)^{-1}(ab)^5a^3b]\ \times$

$[(a^3b(ab)^2a^3b)^{-1}(ab)^5(a^3b(ab)^2a^3b)]\ [a^3b\ (ab)^5\ (a^3b)^{-1}]\ b\ [(a^3b)^{-2}(ab)^5(a^3b)^2]\ b$.

Exercise 23:

Let R = (1234567), moving the pieces around the outside let J = (1234), jumping over the hole. (After each move we move he pieces so that the empty square reverts to its original position.)

The goal is:

g = (17)(26)(35) = (17)(12)(16)(12)(13)(15)(13).

Now RJ = (13)(24567) so $(RJ)^5$ = (13).

We want permutations that fix 1.

Of course $(RJ)^2$ = (25746) fixes 1 and so does R^2J^2 = (35746). Using these together we can map 3 to 7, 2, 6 etc.

$(17) = (R^2J^2)^{-2}(RJ)^5(R^2J^2)^2$;

$(12) = ((R^2J^2(RJ)^{-2})^{-1}(RJ)^5(R^2J^2(RJ)^{-2}$;

$(16) = (R^2J^2)(RJ)^5(R^2J^2)^{-1}$;

$(13) = (RJ)^5$;

$(15) = (R^2J^2)^{-1}(RJ)^5R^2J^2$.

Hence $g = [(R^2J^2)^{-2}(RJ)^{5(}R^2J^2)^2] \times$

$[((R^2J^2(RJ)^{-2})^{-1}(RJ)^5(R^2J^2(RJ)^{-2}] [(R^2J^2)(RJ)^5(R^2J^2)^{-1}] \times$

$[((R^2J^2(RJ)^{-2})^{-1}(RJ)^5(R^2J^2(RJ)^{-2}] \times$

$[(RJ)^5] [(R^2J^2)^{-1}(RJ)^5R^2J^2\ (RJ)^5]$.