THE UNIVERSITY OF SYDNEY

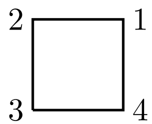
MATH2008 Introduction to Modern Algebra

(http://www.maths.usyd.edu.au/u/UG/IM/MATH2008/)

Semester2, 2003 — Lecturer: R. Howlett

Computer Tutorial 5

This week's computer tutorial explores the symmetries of a square. Think of the vertices of the square as occupying the positions labelled 1, 2, 3 and 4 in following diagram.



The symmetries of the square will be represented by permutations of the set $\{1, 2, 3, 4\}$. The reflection s in the vertical line bisecting the square corresponds to the permutation $(1, 2)(3, 4)$; the reflection t in the diagonal from 2 to 4 corresponds to $(1, 3)$. (Note that the numbers label positions on the paper, and do not move. Think of $(1, 3)$ as saying "move the contents of Location 1 to Location 3, and the contents of Location 3 to Location 1".)

Our first aim is to find out how many symmetries can be constructed just from s and t alone. We can do this by computing things like st, ts, s^2, t^2, $(st)s$, and so on, until we find that we do not get anything new by multiplying together any of the permutations we have already obtained.

In addition to using MAGMA throughout this tutorial you will need to write notes on paper to keep track of the various permutations that arise.

1. The collection of all permutations of $\{1, 2, 3, 4\}$ is a group, called the *symmetric group* Sym(4). Let us call it S for short:
`S := Sym(4);`
The number of elements in a group is called the *order* of the group. Find order of S. (MAGMA denotes it by #S.)

Solution.

```
> S := Sym(4);
> print #S;
24
```

2. Next, tell MAGMA about the permutations s and t described above:

```
s := S!(1,2)(3,4);
t := S!(1,3);
```

Get MAGMA to print these out, to check that you have typed them correctly.

3. Print out various products such as st, ts, s^2, sts, tst and so on. Do pen and paper calculations for at least some of these, and check that you get the same answer as MAGMA. Also, keep track of the different permutations you have created.

Solution.

```
> s := S!(1,2)(3,4);
> t := S!(1,3);
> s*s, s*t, t*s, t*t;
Id(S)
(1, 2, 3, 4)
(1, 4, 3, 2)
Id(S)
```

Because $s^2 = \mathrm{id}$ and $t^2 = \mathrm{id}$, we need only consider products in which s and t alternate: consecutive s's or t's cancel out.

```
> s*t*s, t*s*t, s*t*s*t, t*s*t*s;
(2, 3)
(1, 3)(2, 4)
(1, 4)(2, 3)
(1, 4)(2, 3)
```

Because $stst = tsts$, any alternating product of length greater than 4 equals a product with two consecutive s's or t's, and hence equals something shorter. For example, $ststs = (stst)s = (tsts)s = (tst)s^2 = tst$. So in fact the only permutations you can get from s and t are id, s, t, st, ts, sts, tst and $stst$.

Each of these permutations may be obtained in an infinite number of ways as a product of s's and t's. (For example, $st = s^{2n+1}t$ for any integer n). The key relationships we have discovered are $s^2 = t^2 = \mathrm{id}$ and $stst = tsts$.

4. For each of the permutations you have just created, describe them as symmetries of the square. That is, are they rotations, reflections or something else?

Solution.

id	Identity symmetry operation: does nothing.
$t = (1, 3)$	Reflection in diagonal 24 of square.
$s = (1, 2)(3, 4)$	Reflection in vertical bisector of square.
$ts = (1, 3, 4, 2)$	Clockwise rotation through 90° about centre of square.
$st = (1, 4, 3, 2)$	Anticlockwise rotation through 90° about the centre.
$tst = (1, 4)(2, 3)$	Reflection in horizontal bisector of square.
$sts = (2, 4)$	Reflection in diagonal 13 of square.
$tsts = (1, 3)(2, 4)$	Rotation through 180° about the centre.

5. Has the identity element occurred in your list yet? Keep going until it does.

6. Have you come across the *inverse* of st? How would you recognize it?

Solution.

The identity has come up several times: $s^2 = t^2 = (st)^4 = \mathrm{id}$. The inverse of st can recognised algebraically as the permutation r such that $r(st) = (st)r = e$, or geometrically as the symmetry that reverses the action of st. We observed above that st is the anticlockwise rotation through 90°; its inverse clearly must be clockwise rotation through 90°. The above table tells us that this is ts. You cal get MAGMA to confirm this with `print (t*s)*(s*t);`and `print (s*t)*(t*s);`.

Let X be a set of permutations. We say that X is *closed under multiplication* if it has the property that the product of any two permutations in X is also in X.

Closure: for all pairs (x, y) such that $x, y \in X$, we have $xy \in X$.

(Note that if this property is not satisfied then permutation multiplication does not give us a binary operation on X, since the definition of the term "binary operation" requires that each pair of elements of X gives rise to an element of X. So if X is to form a group under permutation multiplication, it must be closed.)

7. Recall that we are trying to find the smallest set that contains `s` and `t` and is closed under multiplication. Start by defining `X` to be the set containing just `s` and `t`:

```
X := {s,t};
```

Print `X`, to see how MAGMA describes it. Next, use the command

```
print forall{ <x,y> : x in X, y in X | x*y in X };
```

MAGMA will print `true` if it is true for all ordered pairs `<x,y>` with `x,y` in `X` that `x*y` is in `X`, otherwise it will print `false`.

8. Experiment with various other sets, such as `X1 := {s,t,s*t,t*s}` and see if you can find one that contains `s` and `t` and is closed. For example, if `X1` is not closed, try adding an extra element, such as `s*t*s`, and then testing it again. If it is still not closed, add another, and so on.

Solution.

```
> X := {s,t};
> forall { < x,y> : x in X, y in X | x*y in X };
false
> X1 := {s,t,s*t,t*s};
> forall { < x,y> : x in X, y in X1 | x*y in X };
false
> X2 := {id(S),s,t,s*t,t*s};
> forall { < x,y> : x in X, y in X2 | x*y in X };
false
> X3 := {id(S),s,t,s*t,t*s,s*t*s,t*s*t,s*t*s*t};
> forall { < x,y> : x in X, y in X3 | x*y in X };
true
```


Of course, it is clear that we could not hope to get a multiplicatively closed set containing s and t without including at least all of the eight elements listed in the solution to Question 4, since these can all be expressed in terms of s and t. It is nice to have MAGMA's confirmation that these eight elements do form a closed set.

9. Another way to test whether a set such as `X` is closed is to form the set of all products of pairs of elements of `X` and test whether it is a subset of `X`.

```
Y := { x*y : x,y in X };
print Y;
print Y subset X;
```

10. Notice that `Y` does not contain `s` and `t`. So form the union (also called "join") of `X` and `Y` via the command

```
Z := X join Y;
```

and then see whether `Z` is closed. If it is not, form the join of `Z` with the set of all products of pairs of elements of `Z`, and see if that is closed. If not, repeat the process. Will you eventually get to a closed set like this? Try it and see!

Solution.

This must eventually give you a closed set. There are only 24 permutations of $\{1, 2, 3, 4\}$ altogether (see Question 1), and so the sets cannot go on getting bigger indefinitely. When you reach a situation where `ZZ join {x*y : x in ZZ, y in ZZ}` is no bigger than `ZZ` then the set `ZZ` must be closed.

```
> Y:={ x*y : x,y in X};
> Y subset X;
false
> Z:= X join Y;
> {x*y : x,y in Z} subset Z;
false
> Z:= Z join {x*y : x,y in Z};
> {x*y : x,y in Z} subset Z;
true
> Z;
```

```
{
    (1, 3)(2, 4),
    Id(S),
    (1, 2, 3, 4),
    (1, 4, 3, 2),
    (2, 4),
    (1, 3),
    (1, 4)(2, 3),
    (1, 2)(3, 4)
}
```

11. A command `printTable` has been added to MAGMA for this tutorial. `printTable(Z)` prints the multiplication table of the set `Z`. Try it on the sets you have been working with in the previous exercises. Notice that if a product is not in the set, the entry in the table is blank.

Solution.

```
> printTable(X);
Your elements are labelled:
  a: (1, 3)
  b: (1, 2)(3, 4)
and the multiplication table is:
    |  a  b
----+-------
  a |
  b |
A blank entry indicates that the product
is *not* in the original set or sequence.
> Y:=X join {x*y : x,y in X};
> printTable(Y);
Your elements are labelled:
  1: Id($)
  a: (1, 2, 3, 4)
  b: (1, 4, 3, 2)
  c: (1, 3)
  d: (1, 2)(3, 4)
and the multiplication table is:
    |  1  a  b  c  d
----+----------------
  1 |  1  a  b  c  d
  a |  a     1  d
  b |  b  1        c
  c |  c     d  1  b
  d |  d  c     a  1
A blank entry indicates that the product
is *not* in the original set or sequence.
> Z:=Y join {x*y : x,y in Y};
> printTable(Z);
Your elements are labelled:
  1: Id($)
  a: (1, 3)(2, 4)
  b: (1, 2, 3, 4)
  c: (1, 4, 3, 2)
  d: (2, 4)
  e: (1, 3)
  f: (1, 4)(2, 3)
  g: (1, 2)(3, 4)
and the multiplication table is:
```



```
    |  1  a  b  c  d  e  f  g
----+-------------------------
  1 |  1  a  b  c  d  e  f  g
  a |  a  1  c  b  e  d  g  f
  b |  b  c  a  1  f  g  e  d
  c |  c  b  1  a  g  f  d  e
  d |  d  e  g  f  1  a  c  b
  e |  e  d  f  g  a  1  b  c
  f |  f  g  d  e  b  c  1  a
  g |  g  f  e  d  c  b  a  1
A blank entry indicates that the product
is *not* in the original set or sequence.
```

12. By now you should have found a set XX that is closed under multiplication and contains `s` and `t`. Is XX a group? (Does it have an identity element? Does it contain inverses for all of its elements?)

Solution.

Having found a set `XX` such that `printTable(XX)` gives a table with no blank spaces, inspect the table to find out if `XX` contains an x such that $xy = y = yx$ for all y. In fact, it is impossible for a set of permutations of $\{1, 2, \ldots, n\}$ to be closed under multiplication and not contain the identity permutation: `printTable` will denote it by 1. Now to check that every element of `XX` has an inverse in `XX`, check that every row and column of the table contains 1 somewhere. (Again, it is in fact impossible for a multiplicatively closed set of permutations not to have this property.) It is, of course, possible to get MAGMA to search through the set `XX` for an identity element and for inverses for all the elements—some suitable code is given below—but it is more instructive to examine the table yourself.

```
> S:=Sym(4);
> s:=S!(1,2)(3,4);
> t:=S!(1,3);
> X:={s,t};
> Y:= X join {x*y :x,y in X};
> {x*y :x,y in Y} subset Y;
false
> XX:= Y join {x*y :x,y in Y};
> {x*y :x,y in XX} subset XX;
true
> exists { x : x in XX | forall { y : y in XX | x*y eq y}};
true
```

```
> exists(t){ x : x in XX | forall { y : y in XX | x*y eq y}};
true
> t;
Id(S)
> forall { x : x in XX | exists { y : y in XX | (x*y eq t)
>   and (y*x eq t)}};
true
```

For what it is worth, the Math2008 MAGMA startup file `initial.m` defines functions `isClosed`, `hasIdentity` and `hasInverses` that you can use. Thus `hasInverses(XX)` will return `true`.

Since `XX` is closed, permutation multiplication defines an operation on `XX`, and we have now seen that, for this operation, `XX` contains an identity element and inverses for all its elements. The one remaining thing that it must satisfy if it is to be a group is the associative law. It does satisfy this, since it is a general fact that $\rho(\sigma\tau) = (\rho\sigma)\tau$ whenever ρ, σ and τ are permutations of $\{1, 2, \ldots, n\}$. This will be proved in lectures.

13. What is the order of XX? Does XX contain all the symmetries of the square?

Solution.

The elements of XX were listed above; there are eight of them.

```
> #XX;
8
```

Any symmetry of the square will have to move vertex 1 to some vertex i, and there are four choices for i. After i is chosen, vertex 2, being adjacent to vertex 1, will have to be moved to one of the two vertices adjacent to vertex i. Once this choice has been made, the destinations for vertices 3 and 4 are determined automatically. So altogether the number of possibilities is $4 \times 2 = 8$. So XX contains all the symmetries of the square.

14. In the group of symmetries of the square, how many pairs of elements x, y are there such that $xy = yx$?

Hint: the MAGMA expression `x*y eq y*x` is `TRUE` whenever xy equals yx. Now consider the set
`{ <x,y> : x in XX, y in XX | x*y eq y*x }`
(You may read the colon (`:`) as "where" and the vertical line (`|`) as "such that".)

Solution.

```
> #{<x,y> : x in XX, y in XX | x*y eq y*x};
40
> #{{x,y} : x in XX, y in XX | x*y eq y*x};
24
> #{{x,y} : x in XX, y in XX | (x*y eq y*x) and
>    (x ne y)};
16
> #{{x,y} : x in XX, y in XX | (x*y eq y*x) and
>  (x ne y) and (x ne Id(S)) and (y ne Id(S))};
9
```

As you can see, there is a difference between ordered pairs (`<x,y>` in MAGMA) and unordered pairs (`{x,y}`).