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 6

This week's tutorial explores the idea of the *order* of an element and how that relates to the size of the subgroup it generates.

Remember that to print out the value of a variable `x` you use the command `print x;`, or simply `x;`. You should do this rather often.

1. (*i*) Start MAGMA, and enter the five permutations below as elements of the symmetric group Sym(6) (calling them `a`, `b`, `c`, `d` and `e` respectively): $(1,2)(3,4)$, $(1,2,3)$, $(1,2,3,4)(5,6)$, $(1,2,3,4,5,6)$, $(1,2,3)(4,5)$. (To get started, use `G:=Sym(6); a:=G!(1,2)(3,4);`.)

(*ii*) For each of the elements x in (*i*), find all of its powers x, x^2, x^3, x^4, and so on. (Note that you can stop when you get the identity element, since after that the powers will repeat.)

(*iii*) For each of the elements x in (*i*) find all of its powers x^{-1}, x^{-2}, x^{-3}, x^{-4}, and so on.

(*iv*) What do you think that x^0 should be? See if MAGMA agrees.

(*v*) The *order* of x is the least positive integer n such that x^n is the identity. (This is another usage of the word "order": recall that the number of elements in a group is called the order of the group.) What is the order of each of the elements of (*i*)? Do this by using your results from (*ii*), and then check your answers using the MAGMA function `Order`. (You can type `Order(a);` to get the order of `a`.)

(*vi*) The subgroup *generated* by a single element x is the set of all of its powers (positive, negative and zero). If `G` is a group and `x` an element of `G` then the MAGMA command
`H := sub< G | x >;`
constructs the subgroup of `G` generated by `x`. The order of `H` is given by `#H`. Use this to print the orders of the subgroups generated by the elements listed in (*i*).

(*vii*) How do the orders of the subgroups found in (*vi*) compare with the orders of the elements found in (*v*)?

Solution.

```
> S:=Sym(6);
> a:=S!(1,2)(3,4);
> b:=S!(1,2,3);
> c:=S!(1,2,3,4)(5,6);
> d:=S!(1,2,3,4,5,6);
> e:=S!(1,2,3)(4,5);
```

```
> a^2;
Id(S)
> b^2;
(1, 3, 2)
> b^3;
Id(S)
```

```
> c^2;
(1, 3)(2, 4)
> c^3;
(1, 4, 3, 2)(5, 6)
> c^4;
Id(S)
```

Let's use a "for" loop—it's quicker:


```
> for i in [1..7] do d^i;
for> end for;
(1, 2, 3, 4, 5, 6)
(1, 3, 5)(2, 4, 6)
(1, 4)(2, 5)(3, 6)
(1, 5, 3)(2, 6, 4)
(1, 6, 5, 4, 3, 2)
Id(S)
(1, 2, 3, 4, 5, 6)
```

```
> for i in [1..7] do e^i;
for> end for;
(1, 2, 3)(4, 5)
(1, 3, 2)
(4, 5)
(1, 2, 3)
(1, 3, 2)(4, 5)
Id(S)
(1, 2, 3)(4, 5)
```

If x^n is the identity, then $x^{n-1} = x^{-1}$, and $x^{n-2} = (x^2)^{-1} = x^{-2}$, and so on. So looping through the negative powers gives the same elements as obtained by looping through the positive powers, but in the reverse order.

```
> for i in [1..7] do d^(-i);
for> end for;
(1, 6, 5, 4, 3, 2)
(1, 5, 3)(2, 6, 4)
(1, 4)(2, 5)(3, 6)
(1, 3, 5)(2, 4, 6)
(1, 2, 3, 4, 5, 6)
Id(S)
(1, 6, 5, 4, 3, 2)
```

```
> for i in [1..7] do e^(-i);
for> end for;
(1, 3, 2)(4, 5)
(1, 2, 3)
(4, 5)
(1, 3, 2)
(1, 2, 3)(4, 5)
Id(S)
(1, 3, 2)(4, 5)
```

By definition, if G is a group and $x \in G$ then x^0 is the identity element of G.

```
> a^0, b^0, c^0, d^0, e^0;
Id(S)
Id(S)
Id(S)
Id(S)
Id(S)
```

Our calculations above showed that the least positive integer n with $a^n = \mathrm{id}$ is $n = 2$. So the order of a is 2. Similarly b has order 3, c has order 4, and d and e both have order 6.

```
> Order(a), Order(b), Order(c), Order(d), Order(e);
2 3 4 6 6
```

The order of the subgroup generated by x is the same as the order of x, since if x has order n then the subgroup generated by x consists of the n elements $x^0 = \mathrm{id}$, x, x^2, ... , x^{n-1}.

```
> H:=sub< S | a >;
> #H;
2
> H:=sub< S | b >;
> #H;
3
> #sub< S | c>, #sub< S | d >,
  #sub< S | e >;
4 6 6
```

2. (*i*) In each case, use MAGMA to find $x^{-1}yx$:

(a) $x = (1,5,6,3)(2,4)$, $y = (4,6,5)(1,2,3)$;

(b) $x = (1,2)(3,4)$, $y = (1,3)(2,4)$;

(c) $x = (1,3,5,7,9)$, $y = (1,2,3,4)(5,6)$.

(*ii*) Let $x = (1,5,6,3)(2,4)$ and $y = (4,6,5)(1,2,3)$. On a piece of paper write down $1^x, 2^x, 3^x, 4^x, 5^x$ and 6^x. (Remember, 2^x means the number

that x takes 2 to. That is, 2^x is the successor of 2 for the permutation x.) Check that $(4^x, 6^x, 5^x)(1^x, 2^x, 3^x)$ equals $x^{-1}yx$ as found by MAGMA. Repeat for the other two parts of (i).

(iii) If possible, find x so that $x^{-1}yx = z$ where

(a) $y = (1,2)(3,4)$, $z = (1,3)(2,4)$.

(b) $y = (1,2,3)(4,5)$, $z = (1,2)(3,4,5)$.

(c) $y = (1,2,3,4)$, $z = (1,2)(3,4)$.

The expression $x^{-1}yx$ occurs so frequently in group theory that it is given a special name: it is known as the *conjugate* of y by x. MAGMA has a special abbreviation for it, namely `y^x`.

Solution.

(i)

```
> x := S!(1,5,6,3)(2,4);
> y := S!(4,6,5)(1,2,3);
> x^-1*y*x;
(1, 5, 4)(2, 3, 6)
> x := S!(1,2)(3,4);
> y := S!(1,3)(2,4);
```

```
> x^-1*y*x;
(1, 3)(2, 4)
> x := Sym(9)!(1,3,5,7,9);
> y := Sym(9)!(1,2,3,4)(5,6);
> y^x;
(2, 5, 4, 3)(6, 7)
```

Notice that in the last part we had to declare the permutations to be in `Sym(9)` so that we could use a 9 within the permutation x. All the other permutations live happily inside `S` (which still equals `Sym(6)`).

(ii) Remember that 4^x means the number that follows 4 in the cycle of x that contains 4. It is what 4 goes to under x. With $x = (1,5,6,3)(2,4)$, we find that $4^x = 2$, $6^x = 3$, $5^x = 6$, $1^x = 5$, $2^x = 4$ and $3^x = 1$. So $(4^x, 6^x, 5^x)(1^x, 2^x, 3^x) = (2,3,6)(5,4,1)$. It doesn't matter in which order one writes down the disjoint cycles of a permutation, and the cycle $(5,4,1)$ is the same as $(1,5,4)$. So $(2,3,6)(5,4,1) = (1,5,4)(2,3,6)$, which is the answer MAGMA gave for $x^{-1}yx$.

The reason this works is as follows: $y = (4,6,5)(1,2,3)$ means $4^y = 6$, $6^y = 5$, $5^y = 4$, $1^y = 2$, $2^y = 3$, $3^y = 1$. Now if we write $z = x^{-1}yx$ then we have $xz = yx$, and so $(4^x)^z = 4^{xz} = 4^{yx} = (4^y)^x = 6^x$. Similarly $(6^x)^z = (6^y)^x = 5^x$, and so on.

For Part (b), $(1^x, 3^x)(2^x, 4^x) = (2,4)(1,3) = (1,3)(2,4)$.

For Part (c), $(1^x, 2^x, 3^x, 4^x)(5^x, 6^x) = (3,2,5,4)(7,6) = (2,5,4,3)(6,7)$.

(iii) By the principle we have been using, $x^{-1}(1,2)(3,4)x = (1^x, 2^x)(3^x, 4^x)$. We want this to equal $(1,3)(2,4)$. There is more than one possible answer, but the most obvious is to put $2^x = 3$ and $3^x = 2$. So $x = (2,3)$ will do. For the next part we want $(1^x, 2^x, 3^x)(4^x, 5^x) = (1,2)(3,4,5)$. If we write this as $(1^x, 2^x, 3^x)(4^x, 5^x) = (3,4,5)(1,2)$ then it becomes clear that that there is a solution with $1^x = 3$, $2^x = 4$, $3^x = 5$, $4^x = 1$ and $5^x = 2$. That is, $x = (1,3,5,2,4)$. One can get MAGMA to print all the solutions:


```
> p:=S!(1,2,3)(4,5);
> q:=S!(3,4,5)(1,2);
> for x in S do
for> if x^(-1)*p*x eq q then
for|if> print x;
for|if> end if;
for> end for;
```

```
(1, 3, 5, 2, 4)
(1, 4)(2, 5)
(1, 5, 2, 3, 4)
(1, 3, 5)(2, 4)
(1, 4, 2, 5)
(1, 5)(2, 3, 4)
```

For the final part we require $(1^x, 2^x, 3^x, 4^x) = (1,2)(3,4)$. This is impossible to solve, since the left hand side is a 4-cycle and the right-hand side the product of two disjoint 2-cycles.

3. Let `G` be the symmetric group Sym(5).

(i) For each of the numbers n in the sequence `[1..8]` find out how many elements of `G` there are of order n. To get you started, the MAGMA command
`S2:={ x : x in G | Order(x) eq 2 };`
will produce the set of elements of `G` of order 2.

(ii) Is the set `S2` given above a subgroup of `G`?

Solution.

```
> for i in [1..8] do
for> "The number of elements of order",i,"is",
for> #{ x : x in G | Order(x) eq i };
for> end for;
The number of elements of order 1 is 1
The number of elements of order 2 is 25
The number of elements of order 3 is 20
The number of elements of order 4 is 30
The number of elements of order 5 is 24
The number of elements of order 6 is 20
The number of elements of order 7 is 0
The number of elements of order 8 is 0
```

The set `S2` is not a subgroup of `G`. For one thing, it does not contain the identity (which has order 1). For another, it is not closed under multiplication: $(1,2)$ and $(1,3)$ are in `S2`, but $(1,2)(1,3) = (1,2,3)$ is not.

4. What is the smallest symmetric group that has an element of order 15?

Solution.

`Sym(8)` is the smallest symmetric group with an element of order 15. For example, it contains $(1,2,3)(4,5,6,7,8)$. To check that there is no smaller symmetric group containing an element of order 15 we can run the code

```
> for n in [1..8] do
for> print exists{ x : x in Sym(n) | Order(x) eq 15 };
for> end for;
```

(Magma replies false false false false false false false true.)