The University of Sydney

MATH2008 Introduction to Modern Algebra

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

Semester 2, 2003 — Lecturer: R. Howlett

Computer Tutorial 8

The following commands have been introduced in previous tutorials: Sym, Alt, Order, #, forall, exists, sub< G | ... >, PermutationGroup< n | ... >, Set, Stabilizer, diff, meet, join, for ... do ... end for, if ... then ... end if.

1. (*i*) The MAGMA command
F := PermutationGroup< 5 | (1,2,3,4,5), (1,2) >;
creates the smallest group of permutations of the set $\{1,2,3,4,5\}$ that contains $(1,2,3,4,5)$ and $(1,2)$. How many permutations are there in F? And how many permutations of $\{1,2,3,4,5\}$ exist that are *not* in F?

(*ii*) Suppose that the vertices of a regular pentagon are numbered 1, 2, 3, 4, 5. Draw a diagram, and use it to find a permutation a that corresponds to a rotation symmetry of the pentagon, and a permutation b that corresponds to a reflection symmetry. In MAGMA, define D to be the smallest group of permutations containing your permutations a and b. Check that D has order 10. (It is called the *dihedral group of order 10.*)

(*iii*) The *alternating group* of degree n consists of all even permutations of the numbers $1, 2, \dots, n$. The MAGMA command A := Alt(5) creates the alternating group of degreee 5. After doing this, use the command
print D subset A;
to find out whether all the elements of D are even.

(*iv*) Find all the cosets of D in A. Label them D1, D2, ... How many do you expect? (Make sure that your list D1, D2, ... does not contain any repetitions.)

(*v*) For each pair of distinct cosets, find out how many elements they have in common. (If X and Y are sets, their intersection is given by X meet Y.)

(*vi*) To see the elements of A use the command
print Set(A);
Choose any element of A and call it y. Now create some new sets
E1 := { d*y : d in D1 };
E2 := { d*y : d in D2 };
....
and then check that the sets E1, E2 etc. are just the cosets D1, D2, etc. in some order.

(*vii*) Choose two of your cosets—say D2 and D3—and create the set
E := { x*y : x in D2, y in D3 };
Do you expect E to be a coset of D? (First check its size.) Try this again with other cosets in place of D2 and D3.

Solution.

The group F contains all 120 permutations of $1, 2, 3, 4, 5$.

```
> F:= PermutationGroup< 5 | (1,2,3,4,5), (1,2) >;
> #F,#Sym(5);
120 120
> F eq Sym(5);
true
```

If the vertices of the regular pentagon are labelled 1, 2, 3, 4, 5 (cyclically) then $a = (1,2,3,4,5)$ is a rotation symmetry and $b = (2,5)(3,4)$ a reflection symmetry. (Other choices are possible: for example, $(1,3,5,2,4)$ is a rotation and $(1,4)(2,3)$ a reflection.) The permutation group generated by a and b has order 10. Its elements correspond to the five rotation symmetries and five reflection symmetries of the pentagon. (See also Tutorial 7, Question 2.)

The 10 elements of D all lie in the group A = Alt(5), which has order 60. So D is a subgroup of A, and the index of D in A is $60/10 = 6$. That is, there are 6 cosets of D in A.

```
> A:=Alt(5);
> D:=PermutationGroup
 <5|(1,2,3,4,5),(1,4)(2,3)>;
> #A,#D;
60 10
> D subset A;
true
> D1:=Set(D);
> Others:=Set(A) diff D1;
> c:=Random(Others);
> c;
(1, 4, 3)
> D2:={x*c : x in D};
> Others:=Others diff D2;
> d:=Random(Others);
> d;
(2, 4, 5)
> D3:={x*d : x in D};
> Others:=Others diff D3;
> e:=Random(Others);
```

```
> e;
(1, 3, 4, 5, 2)
> D4:={x*e : x in D};
> Others:=Others diff D4;
> f:=Random(Others);
> f;
(1, 4, 3, 5, 2)
> D5:={x*f : x in D};
> Others:=Others diff D5;
> g:=Random(Others);
> g;
(1, 2, 5, 4, 3)
> D6:={x*g : x in D};
> D6 eq Others;
true
> #D1,#D2,#D3,#D4,#D5,#D6;
10 10 10 10 10 10
> Set(A) eq (D1 join D2 join D3
>  join D4 join D5 join D6);
true
```

According to MAGMA, the six sets D1 ... D6 each have 10 elements, and their union is the whole `Set(A)`, which has 60 elements. So they must be disjoint from each other. But rather than simply trusting MAGMA, the student should do at least some calculations by hand and check that the answers agree with MAGMA's.

We can get MAGMA to choose elements of `A` randomly, form the corresponding right cosets of `D`, and check that the result is always one of `D1`, `D2`, ... , `D6`.

```
> z:=Random(A);
> z;
(1, 4, 3, 2, 5)
> E:={x*z : x in D};
> E;
{
    (2, 3)(4, 5),
    (1, 2, 3),
    (2, 4)(3, 5),
    (1, 5, 4),
    (1, 3, 5),
    (1, 4, 2),
    (1, 5, 2, 4, 3),
    (1, 4, 3, 2, 5),
    (1, 3, 4, 5, 2),
    (1, 2, 5, 3, 4)
}
> E in {D1,D2,D3,D4,D5,D6};
true
> z:=Random(A);
> z;
(1, 3, 4, 2, 5)
> E:={x*z : x in D};
> E in {D1,D2,D3,D4,D5,D6};
true
> z:=Random(A);
> z;
(2, 5, 4)
> E:={x*z : x in D};
> E;
{
    (1, 3, 4),
    (1, 4, 5),
    (1, 2, 4, 5, 3),
    (1, 2, 3, 5, 4),
    (2, 4, 3),
    (1, 3)(2, 5),
```



```
    (1, 5)(2, 3),
    (2, 5, 4),
    (1, 4, 3, 5, 2),
    (1, 5, 3, 4, 2)
}
> E in {D1,D2,D3,D4,D5,D6};
true
```

If X, Y are subsets of a group G then we define $XY = \{ xy \mid x \in X, y \in Y \}$. If $X = Hg_1$ and $Y = Hg_2$ are cosets of the subgroup H then it may or may not happen that $(Hg_1)(Hg_2)$ is also a subgroup of H. Note that since $g_1 \in Hg_1$ and $g_2 \in Hg_2$ it is always true that $g_1g2 \in (Hg_1)(Hg_2)$. So if $(Hg_1)(Hg_2)$ is a coset of H then it must be the coset that contains g_1g_2, namely Hg_1g_2. It is reasonably easy to show that $(Hg_1)(Hg_2) = Hg_1g_2$ if and only if $Hg_1 = g_1H$. Certain subgroups, known as *normal* subgroups, satisfy this for all elements $g_1 \in G$. However, the group `D` in our current MAGMA example is not a normal subgroup, and in fact `Dx` is not equal to `xD` unless `x` happens to be in `D`. So it turns out that `D1Di=Di`, for each possible value of `i`, but if `j` $\neq$ `1` then `DjDi` is not one of the cosets. In fact, all these products turn out to have 50 elements.

```
> E:={x*y : x in D2, y in D3};
> #E;
50
> E:={x*y : x in D2, y in D2};
> #E;
50
> E:={x*y : x in D4, y in D6};
> #E;
50
> E:={x*y : x in D1, y in D6};
> #E;
10
> E eq D6;
true
> E:={x*y : x in D5, y in D5};
> #E;
50
```

2. Create the permutation group `G` as follows:

```
G<x,y,z> := PermutationGroup< 9 | (4, 7, 8)(5, 9, 6),
      (3, 6, 9, 4, 5, 7, 8), (1, 3, 2)(4, 7, 8)(5, 6, 9) >;
```

The variables `x`, `y` and `z` will become the given generators. To see this, type

```
print x,y,z;
```

(*i*) Is `G` a subgroup of the alternating group `Alt(9)`? You should be able to answer this without using MAGMA. Or you could use the command `print IsEven(x)` to check each of the generators. Or, then again, you could use the command `print G subset Alt(9);`.

(*ii*) What is the order of G?

(*iii*) Does the order of G divide `#Alt(9)`? What is the reason for this?

(*iv*) How many cosets of G are there in `Alt(9)`?

(*v*) Let K be the stabilizer in G of the set $X = \{1, 2, 3\}$. That is, K consists of the elements $g \in G$ such that 1^g, 2^g and 3^g are 1, 2 and 3 in some order. Use MAGMA to find K by typing
`K := Stabilizer(G,{1,2,3});`
What is the order of K?

(*vi*) Find the stabilizers of a few other subsets of $\{1, 2, \ldots, 9\}$. Check that the order of every subgroup you find divides the order of G.

(*vii*) Does G have a subgroup of order 5? If there is one, find an example; if not, explain why.

(*viii*) Does G have a subgroup of order 4? If there is one, find an example; if not, explain why.

(*ix*) Does G have a subgroup of order 16? If there is one, find an example; if not, explain why.

Solution.

Cycles of odd length are even permutations. In general, a permutation is odd if and only if it has an odd number of cycles of even length. The generators of G do not involve an even length cycles; so they are all even. So G is contained in the alternating group.

```
> G<x,y,z> := PermutationGroup< 9 | (4, 7, 8)(5, 9, 6),
>        (3, 6, 9, 4, 5, 7, 8), (1, 3, 2)(4, 7, 8)(5, 6, 9) >;
> G;
Permutation group G acting on a set of cardinality 9
    (4, 7, 8)(5, 9, 6)
    (3, 6, 9, 4, 5, 7, 8)
    (1, 3, 2)(4, 7, 8)(5, 6, 9)
> G subset Alt(9);
true
> #G;
1512
> #Alt(9)/#G;
120
> K:=Stabilizer(G,{1,2,3});
> #K;
18
```



```
> #G/#K;
84
> #{{1,2,3}^g : g in G};
84
> (9*8*7)/(3*2*1);
84
> L:=Stabilizer(G,{1,2});
> #L;
42
> #G/#L;
36
> #{{1,2}^g : g in G};
36
> (9*8)/(2*1);
36
> M:=Stabilizer(G,{1,2,3,4});
> #M;
12
> #G/#M;
126
> #{{1,2,3,4}^g : g in G};
126
> (9*8*7*6)/(4*3*2*1);
126
> Stabilizer(G,{5,6,7,8,9}) eq M;
true
> Stabilizer(G,{4,5,6,7,8,9}) eq K;
true
> Stabilizer(G,{3,4,5,6,7,8,9}) eq L;
true
```

There are some general facts to note. The stabilizer of a set is always a subgroup. The order of a subgroup of a group is always a divisor of the order of the group: the ratio is called the index of the subgroup. The index of the stabilizer of a set S is equal to the total number of distinct sets you can get by acting on S by elements of the group. Thus, since the stabilizer of $\{1, 2, 3\}$ has index 84 there are 84 distinct sets of the form $\{1^g, 2^g, 3^g\}$, for g in the group G. Each one of these sets occurs for 18 different values of g; this accounts for all elements of G, since $84 \times 18 = 1512$. As it happens, the number of 3-element subsets of $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ is 84, since $\binom{9}{3} = \frac{9\times8\times7}{3\times2\times1} = 84$; so in fact you can get all of these subsets by applying elements of G to $\{1, 2, 3\}$. And so if S_1 and S_2 are any 3-element subsets then there exists an element $x \in G$ with $S_1^x = S_2$: indeed, if $g, h \in G$ are such that $S_1 = \{1^g, 2^g, 3^g\}$ and $S_2 = \{1^h, 2^h, 3^h\}$, then $x = g^{-1}h$ has the desired property.

Similarly, the index of the stabilizer of $\{1,2\}$ is 36; so there are 36 distinct sets of the form $\{1^g, 2^g\}$ with $g \in G$. Each set occurs for 42 different values of g, in agreement with the fact that $36 \times 42 = 1512$. By chance it is again true that the 36 sets of the form $\{1^g, 2^g\}$ are all the 2-element subsets of $\{1,2,3,4,5,6,7,8,9\}$, since $\binom{9}{2} = 36$.

Similarly again, the index of the stabilizer of $\{1,2,3,4\}$ is 126; so there are 126 distinct sets of the form $\{1^g, 2^g, 3^g, 4^6\}$, with $g \in G$. Each set occurs for 12 different values of g, in agreement with the fact that $126 \times 12 = 1512$. Remarkably, it is again true that all 4-element subsets of $\{1,2,3,4,5,6,7,8,9\}$ are obtained like this, $\binom{9}{4}$ happens to equal 126.

The number of 5-element subsets of $\{1,2,3,4,5,6,7,8,9\}$ is the same as the number of 4-element subsets, because the complement of a 5-element subset is a 4-element subset. Because you can get any 4-element subset from any other 4-element set by applying a suitable element of G, you can get any 5-element set from any other by applying a suitable element of G (since if x takes S_1 to S_2 then it also takes the complement of S_1 to the complement of S_2.

Similarly, the fact that you can get any 3-element set from any other by an element of G means that you can get any 6-element set from any other by an element of G. And you can get any 7-element set from any other by an element of G, for the same kind of reason.

Since `#G` is not divisible by 5 or by 16, `G` does not have any subgroup of order 5 or 16. It could have a subgroup of order 4, though. In fact there is a theorem that says that if the order of a group G is divisible by some number that is a power of a prime, then that number is the order of some subgroup of G. Since 4 is a divisor of 1512 and also a power of the prime number 2, there must be a subgroup of order 4. We have already found a subgroup of order 12, and that subgroup will have to have a subgroup of order 4. So let us start by printing out the elements of a subgroup of order 12.

```
> Set(M);
{
    (2, 4, 3)(5, 9, 8),
    (1, 2, 4)(6, 9, 8),
    (1, 4)(2, 3)(5, 9)(6, 8),
    (1, 2, 3)(5, 6, 9),
    (1, 3)(2, 4)(5, 6)(8, 9),
    (1, 3, 4)(5, 8, 6),
    (1, 3, 2)(5, 9, 6),
    (1, 4, 2)(6, 8, 9),
    (1, 2)(3, 4)(5, 8)(6, 9),
```



```
    (1, 4, 3)(5, 6, 8),
    Id(M),
    (2, 3, 4)(5, 8, 9)
}
> N:=sub<M | {g: g in M | Order(g) eq 2}>;
> N;
Permutation group N acting on a set of cardinality 9
    (1, 2)(3, 4)(5, 8)(6, 9)
    (1, 4)(2, 3)(5, 9)(6, 8)
    (1, 3)(2, 4)(5, 6)(8, 9)
> Set(N);
{
    Id(N),
    (1, 2)(3, 4)(5, 8)(6, 9),
    (1, 4)(2, 3)(5, 9)(6, 8),
    (1, 3)(2, 4)(5, 6)(8, 9)
}
```

You can tell the order of a permutation quickly by looking at the lengths of its cycles. In fact, the order is the least common multiple of the lengths of the cycles. So it is easy to see that 8 of the elements of the 12-element group `M` have order 3. No element of order 3 can belong to a subgroup of order 4; so the subgroup of order 4 that we are looking for must consist of exactly the elements of `M` that do not have order 3.