

Dodatek MAGMA Tutorial 1 (just for fun ☺)

In this tutorial you will use MAGMA to calculate the length of vectors and the inner products and distances between vectors. In the course of this you will be introduced to the following MAGMA commands:

```
RealField      VectorSpace      print
func           InnerProduct      Sqrt
Arccos
```

For our purpose, we will use MAGMA calculator from web page:

<http://magma.maths.usyd.edu.au/calc/>

1. Setting up the vector space. Use MAGMA to create a vector space \mathcal{V} of dimension 4 over the real numbers \mathbb{R} . Then define two vectors $(4, 3, 2, 1)^\top$ and $(1, -2, 0, -3)^\top$ named a and b . The commands are

```
R := RealField();
V := VectorSpace(R,4);
a := V![4,3,2,1];
b := V![1,-2,0,-3];
```

Points to note:

- Each statement ends with a semicolon (;). If you press return before you type ; , simply type it on the next line.
- You use := to assign values.
- MAGMA treats vectors as *row* vectors. Also, you need to tell MAGMA which vector space will contain the vector. This is why you use V! before each vector. If you had another vector space, called `mySpace` and of dimension 3, then you would use the command `z:=mySpace![1,2,3]` to create the vector $(1, 2, 3)^\top$ named `z` in the vector space `mySpace`.

Solution.

```
> R := RealField();
> V := VectorSpace(R,4);
> a := V![4,3,2,1];
> b := V![1,-2,0,-3];
```

2. Displaying values. To see the value of the quantities you have defined, you can use the `print` command. For example

```
print a, b;
print V;
```

In fact the word `print` can be omitted if you wish.

Solution.

```
> a, b;
(4 3 2 1)
( 1 -2 0 -3)
> V;
```

Full Vector space of degree 4 over Real Field

3. Inner products and length. You can get these with the following commands:

```
InnerProduct(a,b);
Sqrt(InnerProduct(a,a));
```

(or `print InnerProduct(a,b)` and `print Sqrt(InnerProduct(a,a))`)

Solution.

```
> print InnerProduct(a,b);
-5
> print Sqrt(InnerProduct(a,a));
5.477225575051661134569697828006
```

4. Angles. You should be able to find the angle between a and b using the commands from the previous exercise together with the `Arccos` function. Try this now. You will see that this involves quite a lot of typing and very often you will make typing mistakes. To make things easier, first define an abbreviation for the `Length` function

```
Length := func< v | Sqrt(InnerProduct(v,v)) >;
```

and then define the `Angle` function as

```
Angle := func< u,v | Arccos(InnerProduct(u,v) / (Length(u)* Length(v))) >;
```

Now you can print the angle between a and b using

```
print Angle(a,b);
```

(Notice that `*` is used for multiplication.) The answer will be in radians.

Remark. This is just part of tutorial that we borrowed from following web page:

<http://www.maths.usyd.edu.au/u/bobh/UoS/MATH2008/ctut01.pdf>. Please visit this page for more about this topic.

Dodatek – MAGMA Tutorial¹ 2 (just for fun ☺)

The purpose of this tutorial is to introduce subspaces of vector spaces, to demonstrate how MAGMA can be used to solve matrix equations and how to use matrices to calculate projections and lines of best fit. The MAGMA commands you will learn in this tutorial are:

```
sub          KMatrixSpace   Dimension
Transpose    Solution
```

1. In MAGMA, create the subspace of \mathbb{R}^5 spanned by the vectors $(1, 1, 0, 1, 1)^\top$, $(0, 1, 0, 1, -1)^\top$ and $(3, 1, 0, 1, 5)^\top$. Do this by carrying out the following steps:

- (i) Define the real field $R := \text{RealField}()$; .
- (ii) Create a vector space V of dimension 5 over R and declare the vectors above as a_1 , a_2 and a_3 . For example, $a_1 := V![1, 1, 0, 1, 1]$; .
- (iii) Create the subspace W spanned by a_1 , a_2 and a_3 using the command $W := \text{sub}\langle V | a_1, a_2, a_3 \rangle$; .
- (iv) Find the dimension of W . (Magma has a function `Dimension`)
- (v) Are the vectors a_1 , a_2 and a_3 linearly independent?

Solution.

```
> R := RealField();
> V := VectorSpace(R,5);
> a1 := V![1,1,0,1,1];
> a2 := V![0,1,0,1,-1]; a3 := V![3,1,0,1,5];
> W := sub< V | a1, a2, a3 >;
> Dimension(W);
2
```

Since they span a two-dimensional space rather than a three-dimensional space, a_1 , a_2 and a_3 are linearly dependent.

2. Consider the following vectors in \mathbb{R}^5 : $b_1 = (1, 1, 0, 1, 1)^\top$, $b_2 = (0, 1, 0, 1, 0)^\top$, $b_3 = (-1, 2, -3, 4, -5)^\top$, $v = (1, 5, -4, 3, 6)^\top$. We wish to calculate the projection of v onto the subspace W of \mathbb{R}^5 with basis $\{b_1, b_2, b_3\}$. Since MAGMA uses row vectors rather than column vectors, we will transpose everything.

- (i) We have already (in Exercise 1) created the field R and V , a 5-dimensional space over R . Define $b_1 := V![1, 1, 0, 1, 1]$; and similarly define b_2 , b_3 and v to be the transposes of b_2 , b_3 and v above.
- (ii) Create the vector space of 3×5 matrices using the command $M := \text{KMatrixSpace}(R, 3, 5)$; .
- (iii) Create the matrix B with rows b_1^\top , b_2^\top and b_3^\top using the command $B := M![b_1, b_2, b_3]$; . (This is the transpose of the matrix A whose columns are b_1 , b_2 and b_3).
- (iv) Print B and v to check that you have entered everything correctly, and then define $A := \text{Transpose}(B)$; .
- (v) According to the theory, the projection of v onto W is the vector Ax , where $A^\top Ax = A^\top v$. Taking transposes this equation becomes $x^\top A^\top A = v^\top A$, since transposing reverses multiplication. We can obtain the vector x^\top via the command $x := \text{Solution}(B*A, v*A)$; . (Explanation: if M is a matrix and b a (row) vector then $\text{Solution}(M, b)$ is a vector x that is a solution of the matrix equation $xM = b$.)
- (vi) The projection is $p = Ax$. Transposing (remembering that $B = A^\top$ and that the vector x that MAGMA has found is actually x^\top), we see that $x*B$; will print out the row vector that is the transpose of p .

Solution.

```
> b1 := V![1,1,0,1,1]; b2 := V![0,1,0,1,0];
> b3 := V![-1,2,-3,4,-5];
> M := KMatrixSpace(R,3,5);
> B := M![b1,b2,b3];
> v := V![1,5,-4,3,6]; B,v;
[1 1 0 1 1] [0 1 0 1 0]
[-1 2 -3 4 -5] (1 5 -4 3 6)
> A := Transpose(B);
> x := Solution( B*A, v*A ); x;
(7/2 1/2 0)
> x * B;
(7/2 4 0 4 7/2)
```

¹This is just part of tutorial that we borrowed from following web page: <http://www.maths.usyd.edu.au/u/bobh/UoS/MATH2008/ctut02.pdf>. Please visit this page for more about this topic.

Dodatek – MAGMA Tutorial 3 (just for fun ☺)

This tutorial is about the vector space of polynomials over \mathbb{R} . There is one new MAGMA command you will need to use (PolynomialAlgebra).

Remember that all MAGMA commands end with a semicolon (;) (which can go on the next line, if necessary). You should frequently get MAGMA to print the values of the variables you are working with, to see the results of your actions. (e.g. if you define a subspace by a command like

```
SS := sub< V | u, v >;
```

then you should type `SS;` (or `print SS;`) to find out what MAGMA thinks `SS` is. To see what variables the MAGMA system has defined, type `ShowIdentifiers();`

1. Use MAGMA to add and multiply the polynomials $f(x) = x^7 - 5x^4 + 2x - 1$ and $g(x) = 3x^3 - 2x^2 + x - 1$. To get started type

```
R := RealField();
```

```
P<x> := PolynomialAlgebra(R);
```

(Now MAGMA knows that `P` is the set of all polynomials in the variable `x`.)

(i) The next step is to enter the polynomials themselves. That is,

```
f := x^7 - 5*x^4 + 2*x - 1;
g := 3*x^3 - 2*x^2 + x - 1;
```

(ii) Print out the values of `P`, `f` and `g`.

(iii) Next, print the sum and product of `f` and `g`.

(iv) MAGMA has a function `Eltseq` which returns the sequence of coefficients of a polynomial. To see how it works, type `Eltseq(f);`. Note that the constant term comes first, then the coefficient of x^1 , and so on. You can also define a polynomial by entering its sequence of coefficients, and “coercing” this sequence into the polynomial algebra. Test this by typing `h:=P![-1,1,-2,3];` and then `print h;`

Solution.

```
> R := RealField();
> P<x> := PolynomialAlgebra(R);
> f := x^7 - 5*x^4 + 2*x - 1;
```

```
> g := 3*x^3 - 2*x^2 + x - 1;
> P,f,g;
Univariate Polynomial Ring in x
over Real Field
x^7 - 5*x^4 + 2*x - 1
3*x^3 - 2*x^2 + x - 1
> f+g, f*g;
x^7 - 5*x^4 + 3*x^3 - 2*x^2 + 3*x - 2
3*x^10 - 2*x^9 + x^8 - 16*x^7 + 10*x^6
- 5*x^5 + 11*x^4 - 7*x^3 + 4*x^2 - 3*x + 1
> Eltseq(f);
[ -1, 2, 0, 0, -5, 0, 0, 1 ]
> h:=P![-1,1,-2,3];
> h;
3*x^3 - 2*x^2 + x - 1
> h eq g;
true
```

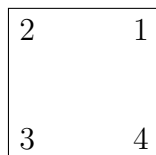
2. If $f(x)$ is a polynomial then the mathematical notation for the number obtained by putting $x = 3$ (say) is $f(3)$. MAGMA has a function `Evaluate` for this: in MAGMA, if `f` is a polynomial then `Evaluate(f,3)` evaluates f at $x = 3$. Evaluate `f`, `g`, `f-g` and `f*g` at $x = 0, 1$ and 10 .
Solution.

```
> Evaluate(f,0); Evaluate(g,0);
-1
-1
> Evaluate(f+g,0); Evaluate(f*g,0);
-2
1
> Evaluate(f,1); Evaluate(g,1);
-3
1
> Evaluate(f+g,1); Evaluate(f*g,1);
-2
-3
> Evaluate(f,10); Evaluate(g,10);
9950019
2809
> Evaluate(f+g,10); Evaluate(f*g,10);
9952828
27949603371
```

Remark. This is just part of tutorial that we borrowed from following web page:
<http://www.maths.usyd.edu.au/u/bobh/UoS/MATH2008/ctut04.pdf>. Please visit this page for more about this topic.

Dodatek – MAGMA Tutorial² 4 (just for fun ☺)

This week's MAGMA 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* $\text{Sym}(4)$. Let us call it S for short: $\mathbf{S} := \text{Sym}(4)$; . The number of elements in a group is called the order of the group. Find order of S . (MAGMA denotes it by $\#\mathbf{S}$.)

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

Remark. Note that in product st MAGMA first compute s , and after that t . How is this different from our initial settings?

```
> 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 $stst$.

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?

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?

²<http://www.maths.usyd.edu.au/u/bobh/UoS/MATH2008/ctut05.pdf>

Dodatek – MAGMA Tutorial³ 5 (just for fun ☺)

We will continue to explore the symmetries of a square, from last time.

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.)

1. 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 :

```
> S := Sym(4); s := S!(1,2)(3,4);  
> t := S!(1,3); 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 xy is in X , otherwise it will print false.

2. Experiment with various other sets, such as $X_1 := \{s, t, st, ts\}$ and see if you can find one that contains s and t and is closed. For example, if X_1 is not closed, try adding an extra element, such as sts , 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 (from last time), 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.

3. 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;
```

4. Notice that Y does not contain s and t . So form the union (also called “join”) of X and Y via the command $Z := X \text{ join } Y$; 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 from last tutorial), 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)}
```

³<http://www.maths.usyd.edu.au/u/bobh/UoS/MATH2008/ctut05.pdf>

Dodatek – MAGMA Tutorial⁴ 6 (just for fun ☺)

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 $\text{Sym}(6)$ (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 “orde”: 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).

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

Let's use a “for” loop—it's quicker:

```
> for i in [1..7] do d^i; 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;
> end for;
```

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);
> 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);
> end for;
```

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;
```

Our calculations above showed that the least positive integer n with $a^n = \text{id}$ 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 $x^0 = \text{id}$, x , x^2 , ..., x^{n-1} .

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

⁴<http://www.maths.usyd.edu.au/u/bobh/UoS/MATH2008/ctut06.pdf>

Dodatek – MAGMA Tutorial⁵ 7 (just for fun ☺)

This week's we will continue to explore the idea of the *order* of an element and how that relates to the size of the subgroup it generates.

2. 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.

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 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:

```
> S:=Sym(6);
> p:=S!(1,2,3)(4,5);
> q:=S!(3,4,5)(1,2);
> for x in S do
>   if x^(-1)*p*x eq q then
>     print x;
>   end if;
> 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 $\text{Sym}(5)$.

(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
>   "The number of elements of order",i,"is",
>   #{ x : x in G | Order(x) eq i };
> 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.

$\text{Sym}(8)$ 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
>   print exists{ x : x in Sym(n)
| Order(x) eq 15 };
> end for;
```

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

⁵<http://www.maths.usyd.edu.au/u/bobh/UoS/MATH2008/ctut06.pdf>

Dodatek – MAGMA Tutorial⁶ 8 (just for fun ☺)

The following commands will be used in today's 8th and next one 9th tutorial: `Sym`, `Alt`, `Order`, `#`, `Set`, `Stabilizer`, `diff`, `meet`, `if ... then ... end if`.

1. Let G be the group of all permutations of $\{1, 2, 3, 4\}$ and let H be the stabilizer of 2 in G . That is, H consists of all permutations in G that leave 2 fixed. These groups can be set up in MAGMA with the commands `G:=Sym(4);`
`H:=Stabilizer(G,2);`

- (i) What are the orders of H and G ?
- (ii) Print all the elements of H . (In MAGMA the command `Set(H)` will produce the elements of H .)
- (iii) Choose any element $y \in G$ and create the set obtained by multiplying every element of H by y (on the right). This is written as Hy and called a right coset of H . The MAGMA command to produce this set and name it C is `C:={h*y:h in H};`
Print C and compare it with H . Is it the same size? Is it the same as H ? How many permutations do they have in common? Does y belong to C ?
- (iv) Choose x in C (with $x \neq y$) and form the coset `D:={h*x:h in H};`
Compare D with C . How many elements do they have in common?
- (v) Is there a common property that the elements of C share? (Hint. Examine 2^x for all x in C .)
- (vi) Now let's be a bit more systematic. We shall create cosets C_1, C_2, \dots , until every element of G is in one of these cosets. Begin by setting C_1 equal to C . The MAGMA command is `C1:=C;`

In MAGMA, if X and Y are sets then `X diff Y` is the set of all elements of X that are not in Y . (Think of "diff" as meaning "different from"). Define

`Z:=Set(G) diff C1;`

and print the elements of Z . Now choose any element of Z (call it y_2) and form the coset `C2:={h*y2:h in H};`

Now redefine `Z:=Z diff C2`, so that now Z consists of the elements that are not in either C_1 or C_2 , choose some y_3 in Z , and form its coset C_3 . Keep going like this until every element of G is in one of your cosets.

- (a) How many cosets do you have?
- (b) What is the size of each of your cosets?
- (c) How much overlap is there between your cosets? (If X and Y are sets, their intersection is given by `X meet Y`.)
- (d) Does the original subgroup H appear in your list of cosets? Why is that?

Solution.

```
> G := Sym(4);
> H := Stabilizer(G,2);
> #G, #H;
24 6
> Set(H);
{
  Id(H),
  (1, 4, 3),
  (3, 4),
  (1, 3, 4),
  (1, 3),
  (1, 4)
}
> y:=G!(1,2);
> C:={ h*y : h in H };
> C;
{
  (1, 3, 4, 2),
  (1, 4, 3, 2),
  (1, 2),
  (1, 4, 2),
  (1, 2)(3, 4),
  (1, 3, 2)
}
> // C, H both have 6 elements
> // y is an element of C
```

Whatever choice you make for the element y , it will always turn out that C has 6 elements, the

⁶<http://www.maths.usyd.edu.au/u/bobh/UoS/MATH2008/ctut07.pdf>

same as H . If y happens to be in H then you will find that $C = H$, otherwise C and H will have no elements in common.

```
> x := G!(1,4,2);
> D := { h*x : h in H };
> D;
{
(1, 4, 3, 2),
...
(1, 2)(3, 4)
}
> D eq C;
true
> for z in C do
for> print 2^z;
for> end for;
1
...
1
```

It will always be the case that $D = C$, no matter which element x in C you choose. This is a general fact about cosets: if H is a subgroup and $C = Hy$ any right coset of H , then $Hx = C$ for all elements $x \in C$.

In this particular example (for the element y that was chosen) the coset C consists of all elements z in G such that $2^z = 1$. There are three other cosets that could have been obtained by choosing y differently:

- (a) the set of all z with $2^z = 2$;
- (b) the set of all z with $2^z = 3$;
- (c) the set of all z with $2^z = 4$.

Observe that the first of these is equal to H (by the definition of H).

```
> C1 := C;
> Z := Set(G) diff C1;
> Z;
{
(2, 3, 4),
(1, 4)(2, 3),
(2, 4),
(1, 3, 4),
(1, 3, 2, 4),
(1, 2, 4, 3),
...
(1, 2, 3),
Id(G),
(1, 4, 3),
(2, 3),
(1, 4)
}
```

```
> y2 := G!(2,3,4);
> C2 := { h*y2 : h in H };
> Z := Z diff C2;
> Z;
{
(1, 3)(2, 4),
(1, 2, 4, 3),
(1, 3, 4),
(1, 4, 3),
(1, 3),
(3, 4),
(1, 2, 4),
(2, 4),
(1, 4),
(1, 3, 2, 4),
Id(G),
(2, 4, 3)
}
> y3 := G!(1,3)(2,4);
> C3 := { h*y3 : h in H };
> Z := Z diff C3;
> Z;
{
Id(G),
(1, 4, 3),
(3, 4),
(1, 3, 4),
(1, 3),
(1, 4)
}
> y4 := Id(G);
> C4 := { h*y4 : h in H };
> Z := Z diff C4;
> Z;
{}
> C1 meet C2, C1 meet C3,
> C1 meet C4;
{}
{}
{}
> C2 meet C3, C2 meet C4,
> C3 meet C4;
{}
{}
{}
> C4 eq Set(H);
true
```

There are four cosets, they have six elements each, and they do not overlap at all. A subgroup is always a right coset of itself: indeed $Hh = H$ whenever h is an element of the subgroup H . In our example the coset C_4 is equal to H .

Dodatek – MAGMA Tutorial⁷ 9 (just for fun ☺)

We will continue where we left last time.

2. Let G be a cyclic group generated by an element of order 12. For example, $G :=$
`PermutationGroup< 12 |`
`(1,2,3,4,5,6,7,8,9,10,11,12) >;` (This is
the same as $G := \text{sub}\langle \text{Sym}(12) \mid$
`(1,2,3,4,5,6,7,8,9,10,11,12)>`).

- (i) Print the elements of G and determine the order of each element.
- (ii) Check that in this group two elements that have the same order always generate the same cyclic subgroup of G .
- (iii) Which elements of G generate all of G ?
Hint: Try the MAGMA code

```
for x in G do
  if sub< G | x > eq G then print x;
end if;
end for;
```

Solution.

```
> G:=PermutationGroup<12|(1,2,3,4,5,6,7,
8,9,10,11,12)>;
> for g in G do
>   print g,"has order",Order(g);
> end for;
Id(G)
has order 1
(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12)
has order 12
(1, 3, 5, 7, 9, 11)(2, 4, 6, 8, 10, 12)
has order 6
..... 10 lines omitted .....
(1, 9, 5)(2, 10, 6)(3, 11, 7)(4, 12, 8)
has order 3
(1, 10, 7, 4)(2, 11, 8, 5)(3, 12, 9, 6)
has order 4
(1, 11, 9, 7, 5, 3)(2, 12, 10, 8, 6, 4)
has order 6
(1, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2)
has order 12
> for x in G do
>   for y in G do
>     if Order(y) eq Order(x) then
```

```
>       print sub <G|x> eq sub <G|y>;
>     end if;
>   end for;
> end for;
true
. . . 27 similar lines omitted . . .
true
```

Since the order of an element is always the same as the order of the cyclic subgroup it generates, an element x in G will generate the whole of G if and only if the order of x is 12. We have already seen that there are exactly four such elements. (They happen to all be 12 cycles.)

```
> for x in G do
>   if sub< G | x > eq G then print x;
>   end if; end for;
(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12)
(1, 6, 11, 4, 9, 2, 7, 12, 5, 10, 3, 8)
(1, 8, 3, 10, 5, 12, 7, 2, 9, 4, 11, 6)
(1, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2)
```

3. The alternating group $\text{Alt}(n)$ consists of all even permutations of $\{1, 2, \dots, n\}$. (A permutation is even if its diagram has an even number of line crossings. An equivalent condition is that the permutation can be expressed as a product of an even number of transpositions (i, j) .) $\text{Alt}(n)$ is a subgroup of $\text{Sym}(n)$ and contains exactly half the elements of $\text{Sym}(n)$.

- (i) Check that for $n = 5$ the alternating group is half the size of the symmetric group. The MAGMA command to create it is $A := \text{Alt}(5);$.
- (ii) For each $n \in \{1, 2, 3, 4, 5, 6\}$, find the number of elements of A of order n .
- (iii) Find two elements of A of order 2 whose product has order 3, and find the order of the subgroup they generate.
- (iv) Find two elements of A of order 2 whose product has order 5, and find the order of the subgroup they generate.
- (v) Find two elements of A of order 2 whose product has order 2, and find the order of the subgroup they generate.

⁷<http://www.maths.usyd.edu.au/u/bobh/UoS/MATH2008/ctut07.pdf>

Dodatek – MAGMA Tutorial⁸ 10 (just for fun ☹)

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, ..., n . The MAGMA command `A:=Alt(5)` creates the alternating group of degree 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 D_1, D_2, \dots . How many do you expect? (Make sure that your list D_1, D_2, \dots 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 E_1, E_2 etc. are just the cosets D_1, D_2 , etc. in some order.

(vii) Choose two of your cosets – say D_2 and D_3 – 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 D_2 and D_3 .

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.

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);
```

⁸<http://www.maths.usyd.edu.au/u/bobh/UoS/MATH2008/ctut08.pdf>

```

> 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 $D1\dots D6$ each have 10 elements, and their union is the whole $\text{Set}(A)$, 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 $D1, D2, \dots, D6$.

```

> 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 $XY = xy|x \in X, y \in Y$. If $X = H_{g_1}$ and $Y = H_{g_2}$ are cosets of the subgroup H then it may or may not happen that $(H_{g_1})(H_{g_2})$ is also a subgroup of H . Note that since $g_1 \in H_{g_1}$ and $g_2 \in H_{g_2}$ it is always true that $g_1g_2 \in (H_{g_1})(H_{g_2})$. So if $(H_{g_1})(H_{g_2})$ is a coset of H then it must be the coset that contains g_1g_2 , namely $H_{g_1g_2}$. It is reasonably easy to show that $(H_{g_1})(H_{g_2}) = H_{g_1g_2}$ if and only if $H_{g_1} = g_1H$. 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

```

Dodatek – MAGMA Tutorial⁹ 11 (just for fun ☺)

We will continue from point where we left last time.

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 $\text{Alt}(9)$? 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 $\#\text{Alt}(9)$? What is the reason for this?

(iv) How many cosets of G are there in $\text{Alt}(9)$?

(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 $\{1, 2, \dots, 9\}$. 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
```

⁹<http://www.maths.usyd.edu.au/u/bobh/UoS/MATH2008/ctut08.pdf>

```

> #{{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 $84 \cdot 18 = 1512$. As it happens, the number of 3-element subsets of $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ is 84, since $\binom{9}{3} = \frac{9 \cdot 8 \cdot 7}{3 \cdot 2 \cdot 1} = 84$; 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 $36 \cdot 42 = 1512$. 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 $\{1^g, 2^g, 3^g, 4^g\}$, with $g \in G$. Each set occurs for 12 different values of g , in agreement with the fact that $126 \cdot 12 = 1512$. 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);
{...
> 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.

Dodatek¹⁰ – MAGMA Tutorial 12 (just for fun ☺)

1. If G is a group and $a \in G$ then the centralizer of a is the set of all elements $g \in G$ that commute with a (meaning that $ag = ga$). Centralizer of an element a is always a subgroup of G .

Let $G = \text{Sym}(11)$, and let $a \in G$ be the 9-cycle $(1, 2, 3, 4, 5, 6, 7, 8, 9)$.

- (i) Use MAGMA to construct the centralizer of a in G . (Define G first, then define the element a , and then use `C:=Centralizer(G,a)` to define the centralizer.)
- (ii) Get MAGMA to print C and the set of elements of C . (MAGMA distinguishes between the group and its set of elements, although mathematicians often do not. Use `Set(C)` to obtain the set.)
- (iii) Define p to be $(2, 4, 5, 10, 11)(3, 6)$ (an element of G), and C_1 to be the coset C_p . Print out the elements of C_1 .
(You can use `C1:={x*p:x in C}`.)
- (iv) Use a for loop to print out the values of $x^{-1}ax$ for all $x \in C_1$.
(You can use `for x in C1 do x^(-1)*a*x; end for;`.)
- (v) You should have noticed something. Can you explain it?
- (vi) Redefine p to be some other element of G - choose any one you like - and repeat the above three parts. Do it for at least 4 different values of p . Have you found an example for which $x^{-1}ax$ is not a 9-cycle? Can you?

Solution.

```
> G:=Sym(11);
> a:=G!(1,2,3,4,5,6,7,8,9);
> C:=Centralizer(G,a);
> C;
Permutation group C acting on a set of
cardinality 11 Order = 18 = 2 * 3^2
```

```
(10, 11)
(1, 2, 3, 4, 5, 6, 7, 8, 9)
> Set(C);
...output omitted... please use MAGMA...
> p:=G!(2,4,5,10,11)(3,6);
> C1:={ c*p : c in C };
> C1;
...output omitted... please use MAGMA...
> for x in C1 do
>   x^(-1)*a*x;
> end for;
...output omitted... please use MAGMA...
> p:=Random(G);
> p;
(1, 9, 5, 3)(2, 7, 10, 11, 6, 4)
> C1:={ c*p : c in C };
> for x in C1 do
>   x^(-1)*a*x;
> end for;
(1, 2, 3, 4, 10, 8, 5, 9, 7)
(1, 2, 3, 4, 10, 8, 5, 9, 7)
. . . 15 lines omitted . . .
(1, 2, 3, 4, 10, 8, 5, 9, 7)
> p:=Random(G);
> p;
(1, 2, 6, 5, 9, 7)(3, 10, 8, 4)
> C1:={ c*p : c in C };
> for x in C1 do
>   x^(-1)*a*x;
> end for;
(1, 4, 7, 2, 6, 10, 3, 9, 5)
(1, 4, 7, 2, 6, 10, 3, 9, 5)
. . . 15 lines omitted . . .
(1, 4, 7, 2, 6, 10, 3, 9, 5)
> p:=Random(G);
> p;
(3, 8, 9)(4, 11, 6, 10)(5, 7)
> C1:={ c*p : c in C };
> for x in C1 do
>   x^(-1)*a*x;
> end for;
(1, 2, 8, 11, 7, 10, 5, 9, 3)
(1, 2, 8, 11, 7, 10, 5, 9, 3)
. . . 15 lines omitted . . .
(1, 2, 8, 11, 7, 10, 5, 9, 3)
```

Observe that when asked to print C MAGMA returned brief but useful information about the group, notably its order and a set of generators. In this case the generators chosen by MAGMA

¹⁰<http://www.maths.usyd.edu.au/u/bobh/UoS/MATH2008/ctut09.pdf>

consist of a 9-cycle and a 2-cycle, which act on disjoint sets: the two fixed points of the second generator are transposed by the first generator, and the nine fixed points of the first generator are cyclically permuted by the second. It follows from this that these generators commute with one another. If we denote the generators by u and t then the 18 elements of C are the 18 elements $u^i c^j$, where $0 \leq i < 2$ and $0 \leq j < 9$. If p is a fixed element of G then the coset Cp consists of the 18 elements of the form cp , where $c \in C$. By the definition of C , each $c \in C$ satisfies $ac = ca$, or (equivalently) $c^{-1}ac = a$. If $x \in Cp$ then $x = cp$ for some $c \in C$, and so $x^{-1}ax = (cp)^{-1}a(cp) = p^{-1}c^{-1}acp = p^{-1}ap$. So all 18 elements $x \in Cp$ give the same value for $x^{-1}ax$.

If $x \in G$ then $x^{-1}(1, 2, 3, 4, 5, 6, 7, 8, 9)x = (1^x, 2^x, 3^x, 4^x, 5^x, 6^x, 7^x, 8^x, 9^x)$. So $x^{-1}ax$ is always a 9-cycle. The total number of 9-cycles in G is $\binom{11}{9}8! = \frac{11!}{18}$, the same as $[G : C]$, the number of distinct right cosets of C in G . Each coset corresponds to a 9-cycle, which is the value of $x^{-1}ax$ for all x in the coset.

2. Set up the following group and find its order.
 $G := \text{PermutationGroup} \langle 9 \mid (1, 2, 3)(7, 8, 9), (1, 2)(3, 4)(5, 6)(7, 8) \rangle;$

Define $x = (1, 2, 3)(7, 8, 9)$ and $y = (1, 2)(3, 4)(5, 6)(7, 8)$, the generators of G .

There is an equivalence relation on $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ such that numbers a and b are equivalent if and only if there is an element $g \in G$ such that $ag = b$. The equivalence classes are called orbits. Two numbers are in the same orbit if you can get from one number to the other in a finite sequence of steps, where each step is to apply either x or y or their inverses. Thus $4^y = 3$ and $3^{x^{-1}} = 2$; so 4 and 2 are in the same orbit.

- (i) Determine whether the following pairs of numbers are in the same orbit of G : 1 and 2; 1 and 5; 2 and 4; 4 and 1; 5 and 8; 8 and 9.
- (ii) The notation a^G is often used for the orbit containing a . Thus, by definition, $a^G = \{a^g : g \in G\}$. To use MAGMA to find the orbit of 3 (for example), you can either type $\{3 \sim g : g \text{ in } G\}$ or $3 \sim G$. In either case you will see the orbit of 3. Try both

commands and then use this method to check your answers to (i) above.

- (iii) For each number i from 1 to 9 find the order of the stabilizer of i in G . Recall that the MAGMA code to produce the stabilizer of 4 in G is $\text{Stabilizer}(G, 4)$.
- (iv) Can you see any relationship between the order of G , the order of the stabilizer of i and the number of elements in the same orbit as i ?
- (v) Let H be the stabilizer of 7 in G .
 - (a) What is the order of H ?
 - (b) How many right cosets of H are there in G ?
 - (c) Let g_1 be an element of G which takes 7 to 8 and let g_2 be an element of G which takes 7 to 9. Use MAGMA to construct the cosets $C_0 := H$, $C_1 := Hg_1$ and $C_2 := Hg_2$. For example,

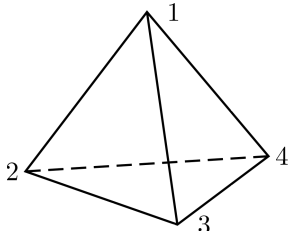
```
> C2 := { h * g2 : h in H };
```
 - (d) Find out where each element of C_1 takes 7. Do the same for C_2 .
 - (e) You already have the answers to the following points in previous parts of this question.
 - (1) What is the orbit of 7?
 - (2) How many cosets does H have in G ?
 - (3) What is the relationship (if any) between the cosets of H and the elements in the orbit of 7?

Solution.

$1^x = 2$; so 1 and 2 are in the same orbit. Since $5^y = 6$ and $6^y = 5$, and x fixes both 5 and 6, you cannot get from 5 to anywhere else but 5 and 6. The orbit containing 5 is $\{5, 6\}$; 1 and 5 are not in the same orbit. Since $4^y = 3$ and $3^{x^{-1}} = 2$, 4 and 2 are in the same orbit. Since 1 and 2 are in the same orbit, and 2 and 4 are in the same orbit, there is no doubt that 1 and 4 are in the same orbit. We have already seen that the orbit containing 5 is $\{5, 6\}$; so 5 and 8 are not in the same orbit. And $8^x = 9$; so 8 and 9 are in the same orbit. (...for exercise type MAGMA code, or visit given link...)

Dodatek – MAGMA Tutorial¹¹ 13 (just for fun ☺)

1. This question is about the group of symmetries of the tetrahedron with vertices labelled 1, 2, 3 and 4 as shown below. Use MAGMA to set up the group $G:=\text{Sym}(4)$ of all permutations of $\{1, 2, 3, 4\}$.



Every rotational symmetry of the tetrahedron corresponds to a permutation of $\{1, 2, 3, 4\}$.

- (i) Find a (nontrivial) rotational symmetry that fixes the vertex 1 and another that fixes the vertex 2, and find the corresponding permutations.
- (ii) Let H be the subgroup of G generated by the permutations you found in Part (i). Get MAGMA to print out all the elements of H , and show that the order of H is 12.
- (iii) Describe each element of H geometrically (e.g. as a rotation about an axis).
- (iv) List the order of each element of H .
- (v) Find a subgroup of H of order 4.

Solution.

Let ℓ_1 be the line through vertex 1 and the central point of the face 234. The rotations about the axis ℓ_1 through 120° and 240° are symmetries of the tetrahedron fixing vertex 1. The corresponding permutations are $(2, 3, 4)$ and $(2, 4, 3)$. Similarly, if ℓ_2 is the line through vertex 2 and the centroid of the face 134 then rotations about ℓ_2 through 120° and 240° are symmetries of the tetrahedron fixing vertex 2. The corresponding permutations are $(1, 3, 4)$ and $(1, 4, 3)$. For Part (i) of the question I chose $(2, 3, 4)$ and $(1, 3, 4)$. There are three other possible choices that would be equally valid.

```
> G:=Sym(4);
> x:=G!(1,3,4);
> y:=G!(2,3,4);
> H:=sub< G | x,y >;
> H;
Permutation group H acting on a set
of cardinality 4
(1, 3, 4)
(2, 3, 4)
> Set(H);
{
(1, 2)(3, 4),
(1, 3, 2),
(1, 3)(2, 4),
(1, 2, 4),
(1, 4, 3),
(1, 3, 4),
(1, 4, 2),
Id(H),
(1, 4)(2, 3),
(2, 4, 3),
(1, 2, 3),
(2, 3, 4)
}
> for t in H do
for> "the order of",t,"is",Order(t);
for> end for;
the order of Id(H) is 1
the order of (1, 3, 4) is 3
the order of (1, 4, 3) is 3
the order of (1, 2, 3) is 3
the order of (2, 3, 4) is 3
the order of (1, 3)(2, 4) is 2
the order of (1, 4, 2) is 3
the order of (1, 2)(3, 4) is 2
the order of (2, 4, 3) is 3
the order of (1, 3, 2) is 3
the order of (1, 4)(2, 3) is 2
the order of (1, 2, 4) is 3
```

Sure enough, H has 12 elements. Four of them have been described above. The permutations $(1, 2, 4)$ and $(1, 4, 2)$ correspond to rotations through 120° and 240° about ℓ_3 , the line joining vertex 3 to the centroid of 124. Similarly, $(1, 2, 3)$ and $(1, 3, 2)$ correspond to rotations through 120° and 240° about ℓ_4 , the line joining vertex 4 to the centroid of 123. The identity is a rotation through 0° (about any axis). The remaining three elements of H are all halfturns:

¹¹<http://www.maths.usyd.edu.au/u/bobh/UoS/MATH2008/ctut10.pdf>

rotations through 180° . For the permutation $(1, 2)(3, 4)$ the axis is the line joining the mid-point of 12 to the midpoint of 34. Similarly, for $(1, 3)(2, 4)$ the axis is the line joining the mid-point of 13 to the midpoint of 24, and for $(1, 4)(2, 3)$ the axis is the line joining the mid-point of 14 to the midpoint of 23.

By Sylow's Theorem H must have a subgroup of order 4, since 4 is the largest power of the prime 2 that is a divisor of 12, the order of H . An element of order k generates a cyclic subgroup of order k , and by Lagrange's Theorem the order of a subgroup has to be a divisor of the order of the group. So the order of any element of a group of order 4 must be a divisor of 4. Now in H there are only four elements whose orders are divisors of 4: the three elements of order 2 and the identity (of order 1). So these four elements are the only ones that can possibly be contained in a group of order 4. But H does have a subgroup of order 4, which certainly contains four elements of H . So it must be these four. So

$$\{id, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$$

is a subgroup of H of order 4.

2. In MAGMA, define G to be the group `Sym(4)`, and define `p1:={{1,4},{2,3}}`;

- (i) How many elements does the set `p1` have? Check your answer with MAGMA. (Use `#p1`;))
- (ii) Define `P:=p1^G`; , and then get MAGMA to print `P`. (Here `p1^G` means the set of everything that `p1` can be changed into by applying a permutation of $\{1, 2, 3, 4\}$.)
- (iii) How many elements does P have? Check your answer with MAGMA (via the command `#P`;)).
- (iv) Each element of P corresponds to a partitioning of the set $\{1, 2, 3, 4\}$ into two subsets of size 2. (Each such partitioning corresponds to a way of pairing up four tennis players for a game of doubles. Thus `p1` above corresponds to players 1 and 4 teaming up against players 2 and 3.) Define now `p2:={{2,4},{1,3}}`; and `p3:={{3,4},{1,2}}`; , so that P is $\{p1, p2, p3\}$. Observe that `p1` is a set with two elements, both of which are themselves sets. And P is a set whose elements are sets whose elements are sets.

- (v) Put `x:=G!(1,4,3,2)`; , and get MAGMA to print `p1^x, p2^x` and `p3^x`. Hence find the permutation of $\{p1, p2, p3\}$ derived from the permutation x of $\{1, 2, 3, 4\}$.
- (vi) Each permutation of $\{1, 2, 3, 4\}$ gives rise to a permutation of $\{p1, p2, p3\}$; so we have a function f from the group of all permutations of $\{1, 2, 3, 4\}$ to the group of all permutations of $\{p1, p2, p3\}$. This function is, in fact, a homomorphism. The MAGMA command


```
f,L,K:=Action(G,P);
```

 defines f to be this homomorphism, L to be the image of f , and K to be the kernel of f . After typing this command, get MAGMA to print f , L and K .
- (vii) Type the MAGMA command `f(x)`; . The response should agree with your answer to Part (v).
- (viii) Find the permutations of $\{p1, p2, p3\}$ corresponding to each of the permutations $(1, 4)$, $(1, 3, 2)$, $(1, 2, 3, 4)$, $(1, 3)$, $(2, 4, 3)$, by using commands such as `f(G!(1,4))`.
- (ix) Find the permutations of $\{p1, p2, p3\}$ corresponding to each of the permutations $(1, 2)(3, 4)$, $(1, 3)(2, 4)$ and $(1, 3)(4, 2)$. Note that these three permutations are all in the group K . Print `Set(K)` to confirm this.
- (x) Put `A:={x*k:k in K}`, and then do the following loop:

```
for t in A do
  f(t);
end for;
```

What do you notice about the answer? Put `B:={G!(1,4)*k:k in K}`, and do a similar for loop. Observe that you again get the same answer four times. Do some more similar loops.

Hints.

```
> p1:={{1,4},{2,3}}; #p1; P:=p1^G; P; #P;
> p2:={{2,4},{1,3}}; p3:={{3,4},{1,2}};
> P eq {p1,p2,p3}; x:=G!(1,4,3,2);
> p1^x,p2^x,p3^x;
> p1^x eq p3, p3^x eq p1, p2^x eq p2; ...
```

Dodatek¹² – MAGMA Tutorial 14 (just for fun ☺)

1. Define $G := \text{Sym}(9)$, and choose any permutations x and y that move only one number in common. For example $x := G!(1, 4, 5, 6)$ and $y := G!(5, 7, 8, 9)$ would do.

- (i) Use MAGMA to compute the permutation $x^{-1}y^{-1}xy$. (You may either type this as it stands or use the MAGMA abbreviation (x, y) for the element $x^{-1}y^{-1}xy$.)
- (i) Repeat this for several other choices of x and y . What do you observe about the result? Try calculating some of the products by hand to see if you can find a reason for what you observe.

Solution.

```
> G:=Sym(9);
> x:=G!(1,2,3)(5,7);
> y:=G!(4,5,8,9);
> (x,y);
(5, 8, 7)
> z:=G!(3,4,6)(8,9);
> (x,z);
(1, 3, 4)
> (z,x);
(1, 4, 3)
> w:=G!(5,8,1,7,2);
> (z,w);
(1, 9, 8)
> (w,z);
(1, 8, 9)
```

The result is always a 3-cycle. Let i be the number that is moved by both x and y , and let $j = i^{x^{-1}}$ and $k = i^x$. Thus j and k are the numbers that appear on either side of i in the expression for x . For example, if $x = (1, 4, 5, 6)$ and $y = (5, 7, 8, 9)$ then $j = 4$, $i = 5$ and $k = 6$. Similarly, let $l = i^{y^{-1}}$ and $m = i^y$. In our example we would have $l = 9$ and $m = 7$. It turns out that $x^{-1}y^{-1}xy$ is actually the 3-cycle (i, m, k) .

As a first step to seeing this, observe that as i is the only number that both x and y move, y fixes

j and k (since x does not fix these two) and x fixes l and m (since y does not). Now consider what $x^{-1}y^{-1}xy$ does to i . Starting from i , apply successively x^{-1} , y^{-1} , x and y :

$$i \xrightarrow{x^{-1}} j \xrightarrow{y^{-1}} j \xrightarrow{x} i \xrightarrow{y} m.$$

Now consider what $x^{-1}y^{-1}xy$ does to m :

$$m \xrightarrow{x^{-1}} m \xrightarrow{y^{-1}} i \xrightarrow{x} k \xrightarrow{y} k.$$

Finally, consider what $x^{-1}y^{-1}xy$ does to k :

$$k \xrightarrow{x^{-1}} i \xrightarrow{y^{-1}} l \xrightarrow{x} l \xrightarrow{y} i.$$

So (i, m, k) is one of the cycles appearing in $x^{-1}y^{-1}xy$. It remains to show that $x^{-1}y^{-1}xy$ fixes everything else.

Choose any number n that is not one of i, m or k . If x and y both fix n then it is clear that $x^{-1}y^{-1}xy$ also fixes n . Now suppose that x moves n , and put $p = n^{x^{-1}}$. Since $n \neq k$, we know that $p \neq k^{x^{-1}} = i$. So neither p nor n is equal to i , and since x moves both p and n it follows that y does not move either p or n . So, on applying $x^{-1}y^{-1}xy$, we find that

$$n \xrightarrow{x^{-1}} p \xrightarrow{y^{-1}} p \xrightarrow{x} n \xrightarrow{y} n.$$

That is, n is fixed by $x^{-1}y^{-1}xy$. Finally, suppose that y moves n , and put $p = n^{y^{-1}}$. Since $n \neq m$, we know that $p \neq m^{y^{-1}} = i$. So neither p nor n is equal to i , and since y moves both p and n it follows that x does not move either p or n . So, on applying $x^{-1}y^{-1}xy$, we find that

$$n \xrightarrow{x^{-1}} n \xrightarrow{y^{-1}} p \xrightarrow{x} p \xrightarrow{y} n.$$

So n is fixed by $x^{-1}y^{-1}xy$ in this case too, and therefore i, m and k are the only things moved by $x^{-1}y^{-1}xy$.

2. Use the following commands to set up subgroups H, K and L of $\text{Alt}(5)$.

```
G := Alt(5);
H := Stabilizer(G,3);
K := Stabilizer(G,4);
L := Stabilizer(G,{3,4});
```

- (i) Find the subgroup M which is the intersection of H and K . Is M a subgroup of L ? (Use the MAGMA command `meet` to get the intersection.)

¹²<http://www.maths.usyd.edu.au/u/bobh/UoS/MATH2008/ctut11.pdf>

(ii) Is M equal to L ? If not, explain why they differ, and how they are related.

Solution.

```
> G := Alt(5);
> H := Stabilizer(G,3);
> K := Stabilizer(G,4);
> L := Stabilizer(G,{3,4});
> L;
Permutation group L acting on a set
of cardinality 5
Order = 6 = 2 * 3
(1, 2)(3, 4)
(2, 5)(3, 4)
> M := H meet K;
> print M subset L;
true
```

This shows that M is a subgroup of L .

```
> Index(L,M);
2
```

This shows that M has just two cosets in L .

The number of elements in M is exactly half the number in L . The elements of L that are not in M interchange 3 and 4, rather than fixing them. Of course, MAGMA can also tell us the order of M and elements that generate M .

```
> M;
Permutation group M acting on a set
of cardinality 5
Order = 3
(1, 5, 2)
```

3(i) Find a set of 3-cycles that generate the alternating group $Alt(5)$. To do this you can set $A:=Alt(5)$ and then check various subgroups of the form

```
sub< A | (1,2,3), . . . >
```

Find a generating set which is as small as possible.

(ii) Repeat Part (i) for $Alt(6)$.

Solution.

```
> A:=Alt(5);
> #A;
60
> x:=A!(1,2,3);
> y:=A!(1,2,4);
> z:=A!(1,2,5);
```

```
> u:=A!(1,3,4);
> v:=A!(1,3,5);
> w:=A!(1,4,5);
> #sub<A|x,y,z,u,v,w>;
60
> #sub<A|x,y>;
12
> #sub<A|x,z>;
12
> #sub<A|x,u>;
12
> #sub<A|x,v>;
12
> #sub<A|x,w>;
60
```

Why do x and w generate $Alt(5)$ while x and y do not? The point is that x and y both fix 5, and so the subgroup generated by x and y is contained in the stabilizer of 5 (which is a subgroup of order 12, isomorphic to $Alt(4)$). Similarly, x and z both fix 4, and hence cannot generate $Alt(5)$. Similar observations hold for the pairs x, u and x, v . But there is no number that is fixed by both x and w .

In view of the above remarks, if we want a set of 3-cycles that generates $Alt(6)$, we had better make sure that between them they move all the numbers 1, 2, 3, 4, 5 and 6. So let us try $(1, 2, 3), (4, 5, 6)$:

```
> A:=Alt(6);
> #A;
360
> #sub<A|A!(1,2,3),A!(4,5,6)>;
9
```

That failed. It failed because $(1, 2, 3)$ and $(4, 5, 6)$ both in the setwise stabilizer of $\{1, 2, 3\}$ (as well as the setwise stabilizer of $\{4, 5, 6\}$). So we will need at least three 3-cycles to generate $Alt(6)$:

```
> #sub<A|A!(1,2,3),A!(4,5,6),A!(1,2,4)>;
360
```

4. Let G be the symmetric group $Sym(5)$ and use MAGMA to construct the following subsets

```
K1:= {G | (1,2), (1,3), (2,3), (2,4),
(2,5), (3,5), (4,5)};
D := { x*G!(1,3,4) : x in
Stabilizer(G,1)};
K2:= Set(G) diff {x*y : x,y in D};
K3:= K1 join K2;...
```

Dodatek – MAGMA Tutorial¹³ 15 (just for fun ☺)

This tutorial explores the groups of rotations of the Platonic solids. The Platonic solids are the five regular polytopes in three dimensions: the tetrahedron, the cube, the octahedron, the icosahedron and the dodecahedron. We shall represent the rotations of these solids as permutations of the vertices. In each case the full group of symmetries is twice as big as the group of rotations (and includes reflections and other kinds of transformations.)

1. The tetrahedron: Set up the group as

```
> T := PermutationGroup< 4 | (1,2,3),  
(1,3,4) >;
```

Check that T has order 12 and is equal to the alternating group $\text{Alt}(4)$. Convince yourself (by looking at the diagram) that the elements of T give all possible rotations of the tetrahedron.

2. The cube: Set up the group as

```
> C:=PermutationGroup< 8 | (1,2,3,4)(8,7,  
6,5), (2,4,6)(7,5,3)>;
```

- (i) Print the elements of C and use the diagram of the cube to work out the correspondence between rotations and permutations. Convince yourself that C contains all possible rotations of the cube.
- (ii) As well as acting on the vertices of the cube the group acts on the four lines through opposite pairs of vertices. To see that the group just permutes these amongst themselves, type the following

```
> pairs := {1,8}^C;  
> pairs;
```

To find the effect of the elements of C on these four pairs of vertices you can type the following:

```
> f,G,K := Action(C,pairs);
```

In carrying out this command MAGMA will construct a homomorphism f from C to the group of permutations of the set

pairs. For each $g \in C$, $f(g)$ is the corresponding permutation. The group G is the image of f and the group K is its kernel.

- (iii) Check that the image of f consists of all permutations of the four pairs and that the kernel contains only the identity element of C . It can be shown that a homomorphism whose kernel consists of the identity element only must be one-to-one. Conclude that the group of rotations of the cube is isomorphic to $\text{Sym}(4)$.
- (iv) If you look at the cube and think hard you should be able to see that there are three pairs of opposite faces and that the rotations of the cube permute these amongst themselves. In this part of the question you will construct a homomorphism from C to the group of permutations of these three pairs of faces. Here is the MAGMA code.

```
> faces := {{1,2,3,4},{5,6,7,8}}^C;  
> print faces;  
> f1,G1,K1 := Action(C,faces);
```

Check that the image of the homomorphism $f1$ is the group of all permutations of the three pairs of faces, and conclude that it is isomorphic to $\text{Sym}(3)$. Do you recognize the kernel?

3. The group of the tetrahedron is isomorphic to $\text{Alt}(4)$ and the group of the cube is isomorphic to $\text{Sym}(4)$. In fact it is possible to place two tetrahedra inside the cube in such a way that the even permutations in $\text{Sym}(4)$ fix the tetrahedra setwise and the odd permutations in $\text{Sym}(4)$ interchange the two tetrahedra. The two tetrahedra are $t_1 = \{2, 4, 6, 8\}$ and $t_2 = \{1, 3, 5, 7\}$.

- (i) Check that every element of C either leaves t_1 in place or sends it to t_2 . Do this with the following MAGMA code.

```
> t1 := {2,4,6,8};  
> for g in C do  
>   t1^g;  
> end for;
```

¹³<http://www.maths.usyd.edu.au/u/bobh/UoS/MATH2008/ctut12.pdf>

- (ii) Use MAGMA to find the stabilizer of t_1 . That is, `>H:=Stabilizer(C,t1)`; What is the order of H ? Is this one of the groups you have seen before? Which one?

4. The Octahedron:

```
> O:=PermutationGroup< 6 | (1,2,3)(4,6,5), (2,3,5,4)>;
```

- (i) Print out the elements of O and convince yourself that all rotations of the octahedron are accounted for.
- (ii) What is the order of O ?
- (iii) Observe that if you put a vertex at the centre of each face, these eight new vertices will describe a cube. Thus the group O must be isomorphic to C , the group of rotations of the cube. Use MAGMA to construct the action of O on its faces:

```
> triples := {1,2,3}~O;
> print triples;
> g, H, L := Action(O,triples);
```

Solutions.

1.

```
> T:=PermutationGroup<4 | (1,2,3),(1,3,4)>;
> #T;
12
```

It is clear that $(1, 2, 3)$ and $(1, 3, 4)$ are rotational symmetries of the tetrahedron, and MAGMA tells us that the group T they generate has order 12. Since $(1, 2, 3)$ and $(1, 3, 4)$ are both even permutations, the group they generate must be a subgroup of the group of all even permutations, $\text{Alt}(4)$. But $\text{Alt}(4)$ has order 12 (since half the 24 permutations of $\{1, 2, 3, 4\}$ are even) and MAGMA tells us that T has order 12; so $T = \text{Alt}(4)$. You can get MAGMA to confirm this: `type T eq Alt(4)`; MAGMA will respond true.

```
> T eq Alt(4);
true
> Set(T);
```

For each vertex of the tetrahedron there are two rotational symmetries that fix that vertex: the line joining the vertex to the centroid of the opposite face is the axis of rotation, and you can rotate through either 120° or 240° . These rotations all have order 3, and correspond to the eight 3-cycles in

$\text{Alt}(4)$. For each edge of the tetrahedron there is a unique opposite edge (joining the two vertices that are not on the given edge). The rotation through 180° about the line joining the midpoints of a pair of opposite edges is a symmetry. This gives three more rotational symmetries. The identity is the 12th. How do we know that there are no more rotational symmetries? Certainly the tetrahedron has some reflection symmetries (six, in fact). For example, the transposition $(1, 2)$ corresponds to the reflection in the plane that is the perpendicular bisector of the edge joining vertices 1 and 2. (Note that vertices 3 and 4 lie in this plane.) Similarly, the other five transpositions in $\text{Sym}(4)$ correspond to reflections in the planes that are the perpendicular bisectors of the other edges. Since every symmetry of the tetrahedron must correspond to some permutation of the vertices, the group of all symmetries must be some subgroup of $\text{Sym}(4)$. So the order of the group of all symmetries must be a divisor of 24. Since we have already geometrically identified 18 symmetries, it follows that the symmetry group of the tetrahedron is the whole of $\text{Sym}(4)$. The six symmetries that we have not yet geometrically identified correspond to the 4-cycles in $\text{Sym}(4)$ (such as $(1, 2, 3, 4)$). If ℓ is the line joining the midpoint of the edge 1-3 with the midpoint of the edge 2-4 then a rotation of 90° about the axis ℓ followed by the reflection in the plane that is the perpendicular bisector of ℓ is a symmetry of the tetrahedron corresponding to a 4-cycle. The other 4-cycles arise similarly.

It is not quite clear that these 4-cycles cannot also be described as rotations in some obscure way. To prove that they are definitely not rotations we need to use some linear algebra. Any rotation of \mathbb{R}^3 fixes all the points on some onedimensional subspace ℓ (the axis of rotation). Let \mathcal{P} be the plane through the origin perpendicular to the line ℓ . Then the rotation acts on \mathcal{P} like a rotation of \mathbb{R}^2 . If we now choose an orthonormal basis of \mathbb{R}^3 made up of one vector on ℓ and two in \mathcal{P} then the matrix of the rotation has the form $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos \theta & -\sin \theta \\ 0 & \sin \theta & \cos \theta \end{pmatrix}$ (where θ

is the angle of rotation). Since this matrix has determinant 1, we conclude that every rotation of \mathbb{R}^3 has determinant 1. A similar analysis can be used to show that reflections have determinant -1. And the transformations that correspond to the 4-cycles also have determinant -1, since they can each be described as the product of one reflection and one rotation. To sum all this up, the 12 even permutations in $\text{Sym}(4)$ (i.e. the elements of $\text{Alt}(4)$) correspond to rotational symmetries, and ...