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

Assignment 2

1. Let $y = (1, 2, 3)(4, 5)$ and $z = (1, 4)(2, 5, 3)$, permutations in Sym(5). Find six distinct permutations $x \in \mathrm{Sym}(5)$ such that $x^{-1}yx = z$.

Solution.

Given that $y = (1, 2, 3)(4, 5)$, it follows that $x^{-1}yx = (1^x, 2^x, 3^x)(4^x, 5^x)$ (for any $x \in \mathrm{Sym}(5)$). This was explained in the solutions to Computer Tutorial 6. The point is that

$$(1^x)^{x^{-1}yx} = 1xx^{-1}yx = 1^{yx} = (1^y)^x = 2^x,$$

since y takes 1 to 2, and by similar calculations

$$(2^x)^{x^{-1}yx} = 2^{yx} = 3^x, \qquad (4^x)^{x^{-1}yx} = 4^{yx} = 5^x,$$
$$(3^x)^{x^{-1}yx} = 3^{yx} = 1^x, \qquad (5^x)^{x^{-1}yx} = 5^{yx} = 4^x.$$

We want $x^{-1}yx = z$; so these equations become $(1^x)^z = 2^x$, $(2^x)^z = 3^x$, $(3^x)^z = 1^x$, $(4^x)^z = 5^x$ and $(5^x)^z = 4^x$. Thus the numbers 1^x, 2^x and 3^x form a 3-cycle in z, while 4^x and 5^x form a 2-cycle. Indeed, z must equal $(1^x, 2^x, 3^x)(4^x, 5^x)$. But $z = (1, 4)(2, 5, 3)$, so $(4^x, 5^x)$ must equal $(1, 4)$ and $(1^x, 2^x, 3^x)$ must equal $(2, 5, 3)$. This means that 4^x is either 1 or 4, and 5^x is either 4 or 1. Similarly 1^x, 2^x, 3^x are 2, 5, 3; it does not matter which is which, but the cyclic ordering must be right. Thus Thus if $1^x = 2$, then $2^x = 5$ and $3^x = 3$, while if $1^x = 5$ then $2^x = 3$ and $3^x = 2$, and if $1^x = 3$ then $2^x = 2$ and $3^x = 5$. So 2 possibilities for 4^x and 5^x multiplied by 3 possibilities for 1^x, 2^x and 3^x makes 6 possibilities for x altogether. They are as follows:

$$4^x = 1, \quad 5^x = 4$$
$$1^x = 2, \quad 2^x = 5, \quad 3^x = 3$$

giving $x = (1, 2, 5, 4)$;

$$4^x = 1, \quad 5^x = 4$$
$$1^x = 5, \quad 2^x = 3, \quad 3^x = 2$$

giving $x = (1, 5, 4)(2, 3)$;

$$4^x = 1, \quad 5^x = 4$$
$$1^x = 3, \quad 2^x = 2, \quad 3^x = 5$$

giving $x = (1, 3, 5, 4)$;

$$4^x = 4, \quad 5^x = 1$$
$$1^x = 2, \quad 2^x = 5, \quad 3^x = 3$$

giving $x = (1, 2, 5)$;

$$4^x = 4, \quad 5^x = 1$$
$$1^x = 5, \quad 2^x = 3, \quad 3^x = 2$$

giving $x = (1, 5)(2, 3)$;

$$4^x = 4, \quad 5^x = 1$$
$$1^x = 3, \quad 2^x = 2, \quad 3^x = 5$$

giving $x = (1, 3, 5)$. It is a routine matter of multiplying permutations to check that

$$\begin{aligned}
(1, 3, 5, 4)^{-1}(1, 2, 3)(4, 5)(1, 3, 5, 4) &= (1, 4)(2, 5, 3),\\
((1, 5, 4)(2, 3))^{-1}(1, 2, 3)(4, 5)(1, 5, 4)(2, 3) &= (1, 4)(2, 5, 3),\\
(1, 2, 5, 4)^{-1}(1, 2, 3)(4, 5)(1, 2, 5, 4) &= (1, 4)(2, 5, 3),\\
(1, 2, 5)^{-1}(1, 2, 3)(4, 5)(1, 2, 5) &= (1, 4)(2, 5, 3),\\
((1, 5)(2, 3))^{-1}(1, 2, 3)(4, 5)(1, 5)(2, 3) &= (1, 4)(2, 5, 3),\\
(1, 3, 5)^{-1}(1, 2, 3)(4, 5)(1, 3, 5) &= (1, 4)(2, 5, 3)
\end{aligned}$$

(and this is all that needs to be done to answer the question).

2. Recall from the inner product space section of the course that an $n \times n$ matrix A is said to be *orthogonal* if $A^T = A^{-1}$. Recall also that $(AB)^T = B^T A^T$.

Show that the set of all orthogonal $n \times n$ matrices is a subgroup of the group of all invertible $n \times n$ matrices by showing that the properties (SG1), (SG2) and (SG3) hold).

Solution.

Let $\mathcal{G}$ be the group of all $n \times n$ invertible matrices and $\mathcal{H}$ the set of all $n \times n$ orthogonal matrices. Then $A \in \mathcal{H}$ if and only if $A^T = A^{-1}$. This certainly implies that every element of $\mathcal{H}$ has an inverse; so $\mathcal{H}$ is a subset of $\mathcal{G}$.

The identity element of G is the $n \times n$ identity matrix I. Since I is its own inverse, and also its own transpose, we have $I^T = I = I^{-1}$, and hence $I \in \mathcal{H}$. So (SG2) holds for $\mathcal{H}$.

Let A, $B \in \mathcal{H}$. Then $A^T = A^{-1}$ and $B^T = B^{-1}$. It was proved earlier in this course that $(AB)^T = B^T A^T$. It is similarly well known that whenever A and B are invertible matrices then their product is invertible, and again the order of the factors is reversed: $(AB)^{-1} = B^{-1}A^{-1}$. So we have that

$$(AB)^T = B^T A^T = B^{-1}A^{-1} = (AB)^{-1},$$

showing that AB is orthogonal. But A and B were arbitrary elements of $\mathcal{H}$; so we have shown that $AB \in \mathcal{H}$ for all A, $B \in \mathcal{H}$. So (SG1) holds for $\mathcal{H}$.

Let $A \in \mathcal{H}$. Then $A^T = A^{-1}$. Transposing this gives $(A^T)^T = (A^{-1})^T$; that is, $A = (A^{-1})^T$. We know that A^{-1} exists, and the inverse of A^{-1} is A (since $AA^{-1} = A^{-1}A = I$). So $(A^{-1})^T = A = (A^{-1})^{-1}$, which shows that $A^{-1} \in \mathcal{H}$. So (SG3) holds for $\mathcal{H}$ too, and so $\mathcal{H}$ is a subgroup of $\mathcal{G}$, as required.

3. Recall that the column vector $\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)$ is an eigenvector of the 2×2 matrix A if and only if $A\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right) = \lambda\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)$ for some scalar λ. Show that the set of all 2×2 invertible matrices A that have $\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)$ as an eigenvector constitutes a subgroup of the group of all invertible 2×2 matrices.

Solution.

Let $\mathcal{G}$ be the group of all 2×2 invertible matrices and

$$\mathcal{H} = \{\mathcal{A} \in \mathcal{G} \mid \mathcal{A}\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right) = \lambda\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right) \text{ for some scalar } \lambda\}.$$

By definition, $\mathcal{H}$ is a subset of $\mathcal{G}$.

The identity element of G is the 2×2 identity matrix I, and since

$$I\begin{pmatrix}1\\1\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix} = \begin{pmatrix}1\\1\end{pmatrix}$$

we see that $I\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right) = \lambda\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)$ holds with $\lambda = 1$. So $I \in \mathcal{H}$; that is, (SG2) holds for $\mathcal{H}$.

Let A, $B \in \mathcal{H}$. Then A and B are invertible 2×2 matrices, and $A\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right) = \lambda\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)$ and $B\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right) = \mu\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)$ for some scalars λ and μ. Since we know (from the Matrix Applications course) that the product of two invertible matrices is invertible, it follows that AB is invertible (with inverse $B^{-1}A^{-1}$), and, moreover,

$$(AB)\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right) = A(B\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)) = A(\mu\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)) = \mu(A\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)) = \mu(\lambda\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)) = (\mu\lambda)\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right).$$

Thus $AB \in \mathcal{H}$ (since $(AB)\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)$ is a scalar multiple of $\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)$). Since A and B were arbitrary elements of $\mathcal{H}$, we have shown that $AB \in \mathcal{H}$ for all A, $B \in \mathcal{H}$. So (SG1) holds for $\mathcal{H}$.

Let $A \in \mathcal{H}$. Then A is invertible and $A\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right) = \lambda\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)$ for some scalar λ. Multiplying both sides by A^{-1} gives

$$\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right) = I\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right) = (A^{-1}A)\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right) = A^{-1}(A\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)) = A^{-1}(\lambda\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)) = \lambda(A^{-1}\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)).$$

This implies that $\lambda \neq 0$ (since $\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right) \neq 0$), and hence $1/\lambda$ exists. Multiplying the above equation by $1/\lambda$ gives

$$\frac{1}{\lambda}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\lambda}\left(\lambda A^{-1}\begin{pmatrix}1\\1\end{pmatrix}\right) = A^{-1}\begin{pmatrix}1\\1\end{pmatrix},$$

showing that $\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)$ is an eigenvector for A^{-1}. Since also A^{-1} is invertible (with inverse A) it follows that $A^{-1} \in \mathcal{H}$. So (SG3) also holds for $\mathcal{H}$, and so $\mathcal{H}$ is a subgroup of $\mathcal{G}$, as required.

4. Start MAGMA and set a log file via the command
`SetLogFile("assign2");`
and then carry out the following steps.

(*i*) Define `S` to be the symmetric group Sym(7).

(*ii*) Define `G` to be the subgroup of S generated by $(1, 7, 6, 5, 4, 3, 2)$ and $(1, 2)(4, 7)$, and find the order of `G`.

(*iii*) Define `C` to be the centralizer of $(1, 7, 6, 5, 4, 3, 2)$ in `G`, and find the order of `C`.

(*iv*) Define `X2` to be the set of elements of `G` of order 2, and find the number of elements in `X2`.

(*v*) Define `X3`, `X4`, `X7` and `X1` to be the sets of elements of `G` of orders 3, 4, 7 and 1 (respectively), and check that along with `X2` these sets account for all elements of `G`.

Solution.

```
> S:=Sym(7);
> a:=S!(1,7,6,5,4,3,2);
> b:=S!(1,2)(4,7);
> G:=sub< S | a,b >;
> #G;
168
> C:=Centralizer(G,a);
> #C;
7
> /* This says that
> there are exactly 7
> elements of G that
> commute with a.
> Since a has order 7
> we know that a has 7
> distinct powers, and
> it is obvious that
> these all commute
> with a. So these are
> the only elements of
> G that commute
> with a. */
```

```
> X2:={ x : x in G | Order(x) eq 2};
> #X2;
21
> X3:={ x : x in G | Order(x) eq 3};
> #X3;
56
> X4:={ x : x in G | Order(x) eq 4};
> #X4;
42
> X7:={ x : x in G | Order(x) eq 7};
> #X7;
48
> X1:={ x : x in G | Order(x) eq 1};
> #X1;
1
> #X1+#X2+#X3+#X4+#X7;
168
> /* Since the sets X1,X2,X3,X4,X7
> obviously have no elements in
> common, and since the total number
> of elements in these sets equals
> the number of elements in G,
> we see that every element of G
> must be in one of these subsets.
> Just to check it another way, we
> can ask magma to confirm that the
> union of these subsets equals the
> whole of G. */
> (X1 join X2 join X3 join X4
> join X7) eq Set(G);
true
```