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

Tutorial 10

1. Four people, whose names are 1, 2, 3 and 4, decide to play a two-against-two partnership game. There are three ways to choose the partnerships: 4 and 1 versus 2 and 3, or 4 and 2 versus 1 and 3, or 4 and 3 versus 1 and 2. Call these three possibilities P_1, P_2 and P_3 respectively. (Thus P_i means that 4 is teamed with i.)

(*i*) Work out the effect of the permutation $\sigma = (1,4,3,2)$ on P_1, P_2 and P_3. (For example, σ changes P_1 from 4&1 versus 2&3 to $4^\sigma\&1^\sigma$ versus $2^\sigma\&3^\sigma$, which is 3&4 versus 1&2 – i.e. P_3.) Thus check that the permutation $(1,4,3,2)$ of the set $\{1,2,3,4\}$ gives rise to the permutation (P_1,P_3) of the set $\{P_1,P_2,P_3\}$.

(*ii*) For each permutation τ of $\{1,2,3,4\}$ let $\phi(\tau)$ be the corresponding permutation of $\{P_1,P_2,P_3\}$. Calculate $\phi(\tau)$ for all 24 permutations τ in $\mathrm{Sym}(4)$.

(*iii*) Note that $(1,4,3,2)(1,4,3) = (1,3,2,4)$. Using the values of $\phi(\tau)$ that you found in Part (*ii*), check that $\phi((1,4,3,2))\phi((1,4,3)) = \phi((1,3,2,4))$. Check that $\phi(\tau)\phi(\rho) = \phi(\tau\rho)$ for a few randomly chosen values of $\tau,\rho \in \mathrm{Sym}(4)$. (Do at least 2 examples.)

(*iv*) The map ϕ described above is an example of a *group homomorphism*; this means simply that ϕ *preserves multiplication*—that is, the equation $\phi(\tau)\phi(\rho) = \phi(\tau\rho)$ holds for all τ and ρ. The *kernel* of ϕ is by definition the set of all τ such that $\phi(\tau)$ is the identity. Find all the elements τ that are in the kernel of ϕ.

(*v*) In fact, $\ker\phi = \{\mathrm{id},(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$. Call this group K. Calculate all 4 elements of the left coset $(1,2)K$, and also calculate all four elements of the right coset $K(1,2)$. (You will find that $(1,2)K = K(1,2)$, since K is what is known as a *normal subgroup* of $\mathrm{Sym}(4)$.) Check that ϕ takes the same value on all 4 elements of this coset. Can you see why this is true? (Hint: it depends on the fact that ϕ is a homomorphism.)

Solution.

The three ways of choosing the partnerships correspond to the three unordered pairs $\{A,B\}$ such that A and B are two-element sets whose union is $\{1,2,3,4\}$. Thus we can identify P_1 with $\{\{4,1\},\{2,3\}\}$, P_2 with $\{\{4,2\},\{1,3\}\}$ and P_3

with $\{\{4,3\},\{1,2\}\}$. Now if $\sigma = (1,4,3,2)$ then

$$
\begin{aligned}
P_2^{\phi(\sigma)} &= P_2^\sigma = \{\{4,2\},\{1,3\}\}^\sigma = \{\{4^\sigma,2^\sigma\},\{1^\sigma,3^\sigma\}\} = \{\{3,1\},\{4,2\}\} = P_2\\
P_3^{\phi(\sigma)} &= P_3^\sigma = \{\{4,3\},\{1,2\}\}^\sigma = \{\{4^\sigma,3^\sigma\},\{1^\sigma,2^\sigma\}\} = \{\{3,2\},\{4,1\}\} = P_1
\end{aligned}
$$

and since also $P_1^{\phi(\sigma)} = P_3$ we see that $\phi(\sigma)$ interchanges P_1 and P_3 and fixes P_2. That is, $\phi(\sigma) = (P_1,P_3)$. See the lecture notes for week 10 for the details of two similar calculations. The complete list of vlues of ϕ is as follows.

$$
\begin{array}{rrr}
\phi(\mathrm{id}) = \mathrm{id} & \phi((1,2,3)) = (P_1,P_2,P_3) & \phi((1,3,2)) = (P_1,P_3,P_2)\\
\phi((1,2)(3,4)) = \mathrm{id} & \phi((2,4,3)) = (P_1,P_2,P_3) & \phi((1,4,3)) = (P_1,P_3,P_2)\\
\phi((1,3)(2,4)) = \mathrm{id} & \phi((1,4,2)) = (P_1,P_2,P_3) & \phi((2,3,4)) = (P_1,P_3,P_2)\\
\phi((1,4)(2,3)) = \mathrm{id} & \phi((1,3,4)) = (P_1,P_2,P_3) & \phi((1,2,4)) = (P_1,P_3,P_2)\\
\phi((1,2)) = (P_1,P_2) & \phi((1,3)) = (P_1,P_3) & \phi((2,3)) = (P_2,P_3)\\
\phi((3,4)) = (P_1,P_2) & \phi((1,4,3,2)) = (P_1,P_3) & \phi((1,2,4,3)) = (P_2,P_3)\\
\phi((1,3,2,4)) = (P_1,P_2) & \phi((2,4)) = (P_1,P_3) & \phi((1,3,4,2)) = (P_2,P_3)\\
\phi((1,4,2,3)) = (P_1,P_2) & \phi((1,2,3,4)) = (P_1,P_3) & \phi((1,4)) = (P_2,P_3)
\end{array}
$$

Let $\sigma = (1,4,3,2)$ and $\tau = (1,4,3)$. Then

$$
\begin{aligned}
(1^\sigma)^\tau &= 4^\tau = 3, & (3^\sigma)^\tau &= 2^\tau = 2,\\
(2^\sigma)^\tau &= 1^\tau = 4, & (4^\sigma)^\tau &= 3^\tau = 1.
\end{aligned}
$$

So $\sigma\tau = (1,3,2,4)$, and (by the table above) $\phi(\sigma\tau) = (P_1,P_2)$. Also by the table, $\phi(\sigma) = (P_1,P_3)$ and $\phi(\tau) = (P_1,P_3,P_2)$. Now

$$
\begin{aligned}
(P_1^{\phi(\sigma)})^{\phi(\tau)} &= P_3^{\phi(\tau)} = P_2\\
(P_2^{\phi(\sigma)})^{\phi(\tau)} &= P_2^{\phi(\tau)} = P_1\\
(P_3^{\phi(\sigma)})^{\phi(\tau)} &= P_1^{\phi(\tau)} = P_3
\end{aligned}
$$

and thus $\phi(\sigma)\phi(\tau) = (P_1,P_2) = \phi(\sigma\tau)$, as claimed.

Here is another example. By the table $\phi((1,2)) = \phi((3,4)) = (P_1,P_2)$, and so

$$\phi((1,2))\phi((3,4)) = (P_1,P_2)(P_1,P_2) = \mathrm{id}.$$

From the table, $\phi((1,2)(3,4)) = \mathrm{id}$, and so $\phi((1,2))\phi((3,4)) = \phi((1,2)(3,4))$. Another: $\phi((2,3)) = (P_2,P_3)$, $\phi((2,4)) = (P_1,P_3)$, $\phi((2,3,4)) = (P_1,P_3,P_2)$. So

$$\phi((2,3))\phi((2,4)) = (P_2,P_3)(P_1,P_3) = (P_1,P_3,P_2) = \phi((2,3,4)) = \phi((2,3)(2,4)).$$

The kernel of ϕ is by definition the set of all $\alpha \in \mathrm{Sym}(4)$ such that $\phi(\alpha)$ is the identity. So according to the table above,

$$\ker\phi = K = \{\mathrm{id},(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}.$$

If $\alpha \in (1,2)K$ then $\alpha = (1,2)\rho$ for some $\rho \in K$, and since ϕ is a homomorphism,

$$\phi(\alpha) = \phi((1,2)\rho) = \phi((1,2))\phi(\rho) = \phi((1,2))\mathrm{id} = \phi((1,2)).$$

So all four elements α in the coset $(1,2)K$ give the same value for $\phi(\alpha)$, namely $\phi(\alpha) = \phi((1,2))$. The same argument shows that $\phi(\alpha) = \phi((1,2))$ for all $\alpha \in K(1,2)$. From the table we see that $\phi((1,2)) = (P_1, P_2)$, and there are just four permutations α such that $\phi(\alpha) = (P_1, P_2)$, namely $(1,2)$, $(3,4)$, $(1,4,2,3)$ and $(1,3,2,4)$. Since $(1,2)K$ must have the same number of elements as K, namely four, it follows that $(1,2)K = \{(1,2),(3,4),(1,4,2,3),(1,3,2,4)\}$. And by the same reasoning, $K(1,2)$ is also this same set. It is straightforward to check this by multiplying permutations: for example, one element of $(1,2)K$ is $(1,2)((1,3)(2,4))$, and calculating this we find that it equals $(1,4,2,3)$.

2. (*i*) List all the elements of $\mathrm{Alt}(4)$, and give the order of each element.

(*ii*) Verify that

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

is a subgroup of $\mathrm{Alt}(4)$.

(*iii*) Show that K is the *only* subgroup of $\mathrm{Alt}(4)$ of order 4.

(Hint: What are the possible orders for an element of a group of order 4?)

Solution.

(*i*) The alternating group, $\mathrm{Alt}(n)$, consists of all even permutations in the symmetric group $\mathrm{Sym}(n)$. Cycles with an odd number of terms are even permutations (see the lecture notes for week 8). In particular, 3-cycles are even. Permutations that are the product of two transpositions are even (since the product of two odd permutations is even). And the identity is even. So the following 12 permutations are even: id, $(1,2)(3,4)$, $(1,3)(2,4)$, $(1,4)(2,3)$, $(1,2,3)$, $(1,3,2)$, $(1,2,4)$, $(1,4,2)$, $(1,3,4)$, $(1,4,3)$, $(2,3,4)$, $(2,4,3)$. If we multiply all 12 of these even permutations by the odd permutation $(1,2)$ we get twelve odd permutations. Since $\mathrm{Sym}(4)$ has only $4! = 24$ elements altogether, the 12 permutations above are the only even permutations in $\mathrm{Sym}(4)$. That is, $\mathrm{Alt}(4)$ consists of the elements above.

Recall that the order of an element g is the least positive k with g^k equal to the identity. It takes 3 applications of a 3-cycle to move things back to where they started. So 3-cycles all have order 3. The identity has order 1. The remaining elements of $\mathrm{Alt}(4)$ are products of disjoint transpositions, and applying such a permutation twice gives the identity. So they all have order 2.

(*ii*) To check by direct calculation that K satisfies (SG1) requires calculating all 16 products $\sigma\tau$ with $\sigma, \tau \in K$, and verifying that the answer is

always in K. The 7 involving the identity are trivial: $\sigma\,\mathrm{id} = \sigma \in K$ for all $\sigma \in K$, and $\mathrm{id}\,\tau = \tau \in K$ for all $\tau \in K$. For each of the three non-identity elements $\sigma \in K$ we find that $\sigma^2 = \mathrm{id} \in K$. (For example $((1,2)(3,4))^2 = \mathrm{id}$.) The remaining 6 cases are very similar to one another, and in fact it turns out that the product (in either order) of two distinct non-identity elements of K gives the third non-identity element. For example,

$$((1,2)(3,4))((1,3)(2,4)) = ((1,3)(2,4))((1,2)(3,4)) = (1,4)(2,3).$$

It follows from these remarks that each element of K is its own inverse; so K satisfies (SG3). We are given that $\mathrm{id} \in K$; so (SG2) holds also.

(*iii*) An element of order k in a group G generates a cyclic subgroup of G of order k, and so by Lagrange's Theorem k must be a divisor of $\#G$. So an element in a group of order 4 must have order 1, 2 or 4. In $\mathrm{Alt}(4)$ there are only 4 elements that have order 1, 2 or 4, since the eight 3-cycles all have order 3. So a subgroup of $\mathrm{Alt}(4)$ of order 4 cannot contain any elements other than these four. Since it has to have four elements–since its order is four—it consists exactly of these elements. Thus K is the only four-element subset of $\mathrm{Alt}(4)$ that can possibly be a subgroup.

This enables us to deduce that K must be a subgroup without directly checking closure under multiplication. Since $\#\mathrm{Alt}(4) = 12$, Sylow's Theorem tells us that $\mathrm{Alt}(4)$ has a subgroup of order 4. So K is this subgroup.

3. Let $A = (a_{ij})$ be a 4×4 matrix. By using the first row expansion formula for the determinant, show that $\det A$ is the sum of 24 terms of the form $\pm a_{1i}a_{2j}a_{3k}a_{4l}$, where i, j, k, l are $1,2,3,4$ in some order. For each such term there is a permutation σ defined by $1^\sigma = i$, $2^\sigma = j$, $3^\sigma = k$, $4^\sigma = l$, and all 24 permutations of $\{1,2,3,4\}$ arise like this. Check that the terms with coefficient -1 correspond to odd permutations, while terms with coefficient $+1$ correspond to even permutations.

Solution.

The determinant of A is equal to

$$a_{11}\begin{vmatrix} a_{22} & a_{23} & a_{24} \\ a_{32} & a_{33} & a_{34} \\ a_{42} & a_{43} & a_{44} \end{vmatrix} - a_{12}\begin{vmatrix} a_{21} & a_{23} & a_{24} \\ a_{31} & a_{33} & a_{34} \\ a_{41} & a_{43} & a_{44} \end{vmatrix} + a_{13}\begin{vmatrix} a_{21} & a_{22} & a_{24} \\ a_{31} & a_{32} & a_{34} \\ a_{41} & a_{42} & a_{44} \end{vmatrix} + a_{14}\begin{vmatrix} a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \\ a_{41} & a_{42} & a_{43} \end{vmatrix}$$

The formula for a 3×3 determinant is

$$\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = a\begin{vmatrix} e & f \\ h & i \end{vmatrix} - b\begin{vmatrix} d & f \\ g & i \end{vmatrix} + c\begin{vmatrix} d & e \\ g & e \end{vmatrix}$$
$$= aei - afh - bdi + bfg + cde - ceg$$

and so det A is as follows:

$$a_{11}(a_{22}a_{33}a_{44} - a_{22}a_{34}a_{43} - a_{23}a_{32}a_{44} + a_{23}a_{34}a_{42} + a_{24}a_{32}a_{43} - a_{24}a_{33}a_{42})$$
$$-a_{12}(a_{21}a_{33}a_{44} - a_{21}a_{34}a_{43} - a_{23}a_{31}a_{44} + a_{23}a_{34}a_{41} + a_{24}a_{31}a_{43} - a_{24}a_{33}a_{41})$$
$$+a_{13}(a_{21}a_{32}a_{44} - a_{21}a_{34}a_{42} - a_{22}a_{31}a_{44} + a_{22}a_{34}a_{41} + a_{24}a_{31}a_{42} - a_{24}a_{32}a_{41})$$
$$-a_{14}(a_{21}a_{32}a_{43} - a_{21}a_{33}a_{42} - a_{22}a_{31}a_{43} + a_{22}a_{33}a_{41} + a_{23}a_{31}a_{42} - a_{23}a_{32}a_{41})$$

Expanding the first line gives 6 terms $\pm a_{1i}a_{2j}a_{3k}a_{4l}$, where $i = 1$ and j, k and l are 2, 3 and 4 in some order. Similarly, the 2nd line gives 6 terms with $i = 2$ and j, k, l equal to 1, 3 and 4 in some order, the third line gives 6 terms with $i = 3$ and $\{j, k, l\} = \{1, 2, 4\}$ and the last line gives 6 terms with $i = 4$ and $\{j, k, l\} = \{1, 2, 3\}$. Each of the 24 terms $a_{1i}a_{2j}a_{3k}a_{4l}$ can be written as $a_{11^\sigma}a_{24^\sigma}a_{34^\sigma}a_{44^\sigma}$ where σ is a permutation of $\{1, 2, 3, 4\}$. For example, $a_{12}a_{24}a_{31}a_{43}$ corresponds to the permutation σ given by $1^\sigma = 2$, $2^\sigma = 4$, $3^\sigma = 1$ and $4^\sigma = 3$. That is, σ takes 1 to 2, 2 to 4, 4 to 3 and 3 to 1, which means that $\sigma = (1, 2, 4, 3)$. The following table lists the permutations associated with the 24 terms in the order in which the terms appear in the expression above:

id	$(3,4)$	$(2,3)$	$(2,3,4)$	$(2,4,3)$	$(2,4)$
$(1,2)$	$(1,2)(3,4)$	$(1,2,3)$	$(1,2,3,4)$	$(1,2,4,3)$	$(1,2,4)$
$(1,3,2)$	$(1,3,4,2)$	$(1,3)$	$(1,3,4)$	$(1,3)(2,4)$	$(1,3,2,4)$
$(1,4,3,2)$	$(1,4,2)$	$(1,4,3)$	$(1,4)$	$(1,4,2,3)$	$(1,4)(2,3)$

Recall that cycles with an even number of terms are odd permutations. The 6 transpositions and the 6 four-cycles are thus odd, and since there are exactly 24 permutations of $\{1, 2, 3, 4\}$ we know that 12 of them are even and 12 are odd. So the transpositions and the 4-cycles are the only odd permutations of $\{1, 2, 3, 4\}$. Looking back at the original expression, we see that the terms with minus signs are exactly the ones that correspond to odd permutations: the 2nd, 3rd and 6th terms in the first and third rows, and the 1st, 4th and 5th terms in the second and last rows.

4. (*i*) Let G be a finite group and let H be a nonempty subset of G satisfying ($SG1$) (closure). Show that H automatically satisfies ($SG2$) and ($SG3$).

(*ii*) Find an *infinite* group G and a nonempty subset H of G such that H satisfies ($SG1$) but neither ($SG2$) nor ($SG3$).

Solution.

(*i*) Suppose that H is closed and $a \in H$. The elements a, a^2, a^3, ... cannot be all distinct, since G is finite. So there exist positive integers r, s with $r > s$ and $a^r = a^s$. Multiplying this equation by $(a^{-1})^s$ gives $a^{r-s} = e$ (identity). Since H is closed under multiplication and $a \in H$, it follows that $a^k \in H$ for all $k > 0$. In particular, $a^{r-s} \in H$. That is, $e \in H$. So H satisfies (SG2).

We have shown that there exists a positive integer n such that $a^n = e$. If $n = 1$ then $a = e = a^{-1}$, and so $a^{-1} \in H$. If $n > 1$ then $n - 1 \geq 1$, and so $a^{n-1} \in H$ (by closure). Since $a(a^{n-1}) = (a^{n-1})a = e$ we see that $a^{n-1} = a^{-1}$, and so $a^{-1} \in H$. So H satisfies (SG3).

(*ii*) Take G to be $\mathbb{Z}$ (integers) under addition. Let $H = \{1, 2, 3, \dots\}$, the positive integers. Then H is closed under addition: (SG1) holds. But $0 \notin H$; so (SG2) does not hold. And $1 \in H$ while $-1 \notin H$; so (SG3) does not hold.

5. Let $f \in \mathrm{Sym}(n)$ and $1 \leq m \leq n$. The permutation f takes the numbers 1, 2, ..., m to some other numbers 1^f, 2^f, ..., m^f. Show that the set

$$K = \{\, f \in \mathrm{Sym}(n) \mid \{1, 2, \dots, m\} = \{1^f, 2^f, \dots, m^f\}\,\}$$

is a subgroup of $\mathrm{Sym}(n)$. (We call K the *setwise stabilizer* of $\{1, \dots, m\}$. Although a permutation in K maps this set to itself, it need not fix any of the numbers individually.) Find the order of K, and deduce that $m!(n-m)!$ is a divisor of $n!$. (Use Lagrange's Theorem.)

Solution.

Observe that for all permutations f, the set $\{1^f, 2^f, \dots, m^f\}$ has the same number of elements as $\{1, 2, \dots, m\}$. So $\{1^f, 2^f, \dots, m^f\} = \{1, 2, \dots, m\}$ if and only if $i^f \in \{1, 2, \dots, m\}$ for all $i \in \{1, 2, \dots, m\}$. Thus it follows that $K = \{\, f \in \mathrm{Sym}(n) \mid i^f \in M \text{ for all } i \in M\,\}$.

Let f, $g \in K$, and let $i \in M$. Then $i^f \in M$ (since $f \in K$) and so $(i^f)^g \in M$ (since $g \in K$). Thus $i^{(fg)} = (i^f)^g \in M$ for all $i \in M$. Thus $fg \in K$. This holds for all f, $g \in K$; so K satisfies (SG1) (closure under multiplication).

Obviously $i^{\mathrm{id}} = i \in M$ for all $i \in M$. So $\mathrm{id} \in K$. So K satisfies (SG2).

Let $f \in K$ and $i \in \{1, 2, \dots, m\}$. Since $\{1, 2, \dots, m\} = \{1^f, 2^f, \dots, m^f\}$, there exists $j \in M$ such that $i = j^f$. So $i^{f^{-1}} = j \in M$. Since i was an arbitrary element of M, we have shown that $i^{f^{-1}} \in M$ for all $i \in M$. So $f^{-1} \in K$. Hence K satisfies (SG3) (closure under forming inverses).

An element of K consists of a permutation of M (a set of size m) together with a permutation of $\{1, \dots, n\} \setminus M$ (a set of size $n - m$). There are $m!$ possibilities for the former and $(n - m)!$ for the latter; so $\#K = m!(n - m)!$. Lagrange's Theorem states that the order of a subgroup of a finite group is always a divisor of the order of the group. Since K is a subgroup of $\mathrm{Sym}(n)$ and $\#\mathrm{Sym}(n) = n!$ it follows that $m!(n - m)!$ divides $n!$. (Of course we already knew this since the binomial coefficient $\binom{n}{m}$ is an integer and equals $\frac{n!}{m!(n-m)!}$.)