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 9

1. Let G be a cyclic group generated by an element a of order 50.

(i) Find the orders of all the elements of G.

(ii) List the elements of G that form a subgroup of order 10.

(iii) Prove that a^{13k} equals the identity if and only if k is a multiple of 50. Deduce that a^{13} generates G.

(iv) Find a value of k such that $a^{13k} = a$.

(v) Find all the elements of G of order 10.

(vi) Show that a^5 can be expressed as a power of a^{35}.

Solution.

(i) The order of a^n is the least positive integer k such that $a^{nk} = e$. This is the least positive integer k such that nk is a multiple of 50. So if k is the order of a^n then nk is least common multiple of n and 50. Thus we obtain the following formula:

$$\text{Order}(a^n) = \frac{\text{lcm}(n,50)}{n}. \qquad (1)$$

For example, consider the case $n = 4$. The lcm of 4 and 50 is the first term in the sequence 4, 8, 12, 16, 20, … that is divisible by 50. It is easy to see that this is 100. So the order of a^4 is $\frac{100}{4} = 25$. Similarly, to find the order of a^{35} we can look at the sequence of multiples of 35, namely 35, 70, 105, 140, 175, … , and find the first one that is a multiple of 50. It is not hard to see that the answer is 350. (Alternatively, one can look at the sequence of multiples of 50 and find the first one that is divisible by 35.) So the order of a^{35} is $\frac{350}{35} = 10$.

If d is an integer that is a divisor of both 50 and n then $\frac{n}{d}$ and $\frac{50}{d}$ are both integers, and so the number $\frac{n}{d}50 = n\frac{50}{d}$ is a multiple of both n and 50. The least common multiple of n and 50 is found by taking d to be the greatest common divisor of n and 50. That is,

$$\text{lcm}(n,50) = \frac{50n}{\gcd(n,50)}.$$

Using this the equation (1) above can be rewritten as

$$\text{Order}(a^n) = \frac{50}{\gcd(n,50)}. \qquad (2)$$

For any given value of n between 1 and 50, it is very easy to determine the gcd of n and 50: the only divisors of 50 are 1, 2, 5, 10, 25 and 50,

and one can quickly find the largest one of these that is a divisor of n. The gcd of n and 50 is 1 for the following values of n: 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47 and 49. So a^1, a^3, a^7, etc. all have order 50. The gcd of n and 50 is 2 for the following values of n: 2, 4, 6, 8, 12, 14, 16, 18, 22, 24, 26, 28, 32, 34, 36, 38, 42, 44, 46 and 48. The corresponding powers of a all have order $\frac{50}{2} = 25$. The gcd of n and 50 is 5 for $n = 5$, 15, 35, 45. The corresponding powers of a have order $\frac{50}{5} = 10$. The gcd of n and 50 is 10 for $n = 10$, 20, 30, 40; so a^{10}, a^{20}, a^{30} and a^{40} have order 5. Finally, a^{25} has order 2 and a^{50} has order 1.

(ii) The powers of a^5 clearly form a subgroup of order 10. The elements of this subgroup are a^5, a^{10}, a^{15}, a^{20}, a^{25}, a^{30}, a^{35}, a^{40}, a^{45} and $a^{50} = e$. Note that all the elements of order 10 lie in this subgroup. It is in fact the only subgroup of G of order 10.

(iii) Since $\gcd(13,50) = 1$, $13k$ is divisible by 50 if and only if k is divisible by 50. That is, a^{13} has order 50 (as we already noted above). So the subgroup of G generated by a^{13} must have 50 elements. But G itself only has 50 elements; so a^{13} generates the whole of G. The successive powers of a^{13} are a^{13}, a^{26}, a^{39}, $a^{52} = a^2$, a^{15}, a^{28}, a^{41}, $a^{54} = a^4$, a^{17}, … . Continuing this process we find that we get a^1 after 27 steps. (Alternatively, one can find the smallest number of the form $50k + 1$ that is a multiple of 13. It is $351 = 13 \times 27$.)

(iv) See Part *(iii)*.

(v) $(a^{35})^3 = a^{105} = a^5$.

2. Let G be a group and let $\sim$ be the relation on G defined as follows: for all x, $y \in G$,

$$x \sim y \text{ if and only if } x = t^{-1}yt \text{ for some } t \in G.$$

Prove that $\sim$ is an equivalence relation. (This relation is called *conjugacy.* If $x \sim y$ then x and y are said to be *conjugate.* The equivalence classes are called *conjugacy classes.*)

Solution.

Let e be the identity element of G. For all $x \in G$, $x = exe = e^{-1}xe$ (since $e = e^{-1}$). This shows that $x \sim x$, for all $x \in G$. So the relation $\sim$ is reflexive.

Suppose that x, $y \in G$ with $x \sim y$. Then $x = t^{-1}yt$ for some $t \in G$. This equation gives

$$txt^{-1} = tt^{-1}ytt^{-1} = eye = y;$$

that is, $y = u^{-1}xu$, where $u = t^{-1}$. Hence $y \sim x$. So we have shown that $y \sim x$ whenever $x \sim y$; that is, $\sim$ is symmetric.

Suppose that x, y, $z \in G$ with $x \sim y$ and $y \sim z$. Then there exist t, $u \in G$ with $x = t^{-1}yt$ and $y = u^{-1}zu$. Substituting the second of these equations into the first gives $x = t^{-1}(u^{-1}zu)t = (ut)^{-1}z(ut)$ (since $(ut)^{-1} = t^{-1}u^{-1}$).

Hence $x \sim z$. Since this holds whenever $x \sim y$ and $y \sim z$, we have shown that $\sim$ is transitive.

3. Let $G = \mathrm{Sym}(3)$, and consider the conjugacy relation $\sim$ defined in Question 2.

(i) Show that $(1,2,3) \sim (1,3,2)$ and $(1,2) \sim (2,3)$.

(ii) Find all the conjugacy classes in G.

Solution.

(i) Recall that $x^{-1}(1,2,3)x = (1^x, 2^x, 3^x)$. (See Question 2 of Computer Tutorial 6.) If we put $x = (2,3)$ then $1^x = 1$, $2^x = 3$ and $3^x = 2$, and so $x^{-1}(1,2,3)x = (1,3,2)$. Thus $(1,3,2) \sim (1,2,3)$, as required.

Similarly, $x^{-1}(1,2)x = (1^x, 2^x)$, and we can ensure that this equals $(2,3)$ by choosing x to be such that $1^x = 2$, $2^x = 3$ and $3^x = 1$. So $(1,2) \sim (2,3)$.

(ii) We have shown in Part (i) that $(1,2) \sim (2,3)$, and it is equally easy to show that $(1,2) \sim (1,3)$. So all three 2-cycles in $\mathrm{Sym}(3)$ are conjugate to one another. Since $x^{-1}(1,2)x = (1^x, 2^x)$, we see that any conjugate of $(1,2)$ has to be a 2-cycle; so there are no other elements in this conjugacy class. So the three 2-cycles $(1,2)$, $(2,3)$, $(1,3)$ form one of the conjugacy classes of G. Similarly, since $x^{-1}(1,3,2)x = (1^x, 2^x, 3^x)$, any conjugate of $(1,3,2)$ has to also be a 3-cycle. There are only two 3-cycles in $\mathrm{Sym}(3)$, and we showed in Part (i) that they are conjugate. Thus $(1,2,3)$, $(1,3,2)$ form a conjugacy class in G. The one remaining element of G is the identity, which is not conjugate to anythingbut itself. Thus G has exactly three conjugacy classes:

$$\{\mathrm{id}\}, \quad \{(1,2),(2,3),(1,3)\}, \quad \{(1,2,3),(1,3,2)\}.$$

4. Let G be a group and $y \in G$. Show that the set

$$C_G(y) = \{\, x \in G \mid x^{-1}yx = y \,\}$$

is a subgroup of G. (The subgroup $C_G(y)$ is called the *centralizer* of y in G.) Show that if t, $u \in G$ are such that $t^{-1}yt = u^{-1}yu$ then $tu^{-1} \in C_G(y)$, and hence $t \in C_G(y)u$. Does it follow that $u \in C_G(y)t$?

Solution.

Let a, $b \in C_G(y)$. Then $a^{-1}ya = y$ and $b^{-1}yb = y$. So

$$(ab)^{-1}y(ab) = b^{-1}a^{-1}yab = b^{-1}(a^{-1}ya)b = b^{-1}yb = y,$$

from which it follows that $ab \in C_G(y)$. We have shown that ab is in $C_G(y)$ whenever a and b are in $C_G(y)$. Thus $C_G(y)$ satisfies (SG1).

If e is the identity element of G then we have $e^{-1} = e$, and

$$e^{-1}ye = e(ye) = ey = y.$$

This shows that $e \in C_G(y)$. Thus $C_G(y)$ satisfies (SG1).

Let $a \in C_G(y)$. Then $y = a^{-1}ya$, and so

$$aya^{-1} = a(a^{-1}ya)a^{-1} = (aa^{-1})y(aa^{-1}) = eye = y.$$

Thus $(a^{-1})^{-1}ya^{-1} = y$, which shows that $a^{-1} \in C_G(y)$. Since this holds whenever $a \in C_G(y)$, we have shown that $C_G(y)$ satisfies (SG3). So $C_G(y)$ is a subgroup of G.

If $t^{-1}yt = u^{-1}yu$ then $ut^{-1}ytu^{-1} = uu^{-1}yuu^{-1} = eye = y$. That is, if $t^{-1}yt = u^{-1}yu$ then $(tu^{-1})^{-1}y(tu^{-1}) = y$, and this says that $tu^{-1} \in C_G(y)$.

If $tu^{-1} \in C_G(y)$, then the equation $t = (tu^{-1})u$ shows that $t \in C_G(y)u$.

We have just shown that if $t^{-1}yt = u^{-1}yu$ then $t \in C_G(y)u$. Our hypothesis here is not altered by swapping t and u: the equations $t^{-1}yt = u^{-1}yu$ and $u^{-1}yu = t^{-1}yt$ say the same thing. So the argument that proves $t \in C_G(y)u$ also proves that $u \in C_G(y)t$ (just by swapping t and u at every step).

5. Let $y = (1,2,3) \in \mathrm{Sym}(4)$, and let C be the centralizer of y in $\mathrm{Sym}(4)$.

(i) Find all the elements of C.

(ii) Find all the elements of the coset $C(3,4)$.

(iii) Find all the elements $x \in G$ such that $x^{-1}yx = (1,2,4)$.

Solution.

Note that since we are dealing with $\mathrm{Sym}(4)$, the permutation $(1,2,3)$ is really $(1,2,3)(4)$: the number 4 is a 1-cycle, or fixed point, of y. Remember also that any of the numbers in a cycle can be written first: $(2,3,1)$ and $(3,1,2)$ are both the same as $(1,2,3)$. Thus $y = (1,2,3)(4) = (2,3,1)(4) = (3,1,2)(4)$.

(i) If x is an element of $\mathrm{Sym}(4)$, then $x \in C$ if and only if $x^{-1}yx = y$. That is, $x \in C$ if and only if $x^{-1}(1,2,3)(4)x = (1,2,3)(4)$. Now, as we saw in Question 2 of Computer Tutorial 6, $x^{-1}(1,2,3)(4)x = (1^x, 2^x, 3^x)(4^x)$. So $x \in C$ if and only if

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

We see that there are three solutions. They are

$$\begin{aligned}
&1^x = 1, \quad 2^x = 2, \quad 3^x = 3, \quad 4^x = 4, \quad \text{giving } x = \mathrm{id};\\
&1^x = 2, \quad 2^x = 3, \quad 3^x = 1, \quad 4^x = 4, \quad \text{giving } x = (1,2,3)(4);\\
&1^x = 3, \quad 2^x = 1, \quad 3^x = 2, \quad 4^x = 4, \quad \text{giving } x = (1,3,2)(4).
\end{aligned}$$

Thus the three elements of C are id, $(1,2,3)$ and $(1,3,2)$.

(ii) The three elements of $C(3,4)$ are $\mathrm{id}(3,4)$, $(1,2,3)(3,4)$ and $(1,3,2)(3,4)$. Thus

$$C(3,4) = \{(3,4), (1,2,4,3), (1,4,3,2)\}.$$

(iii) We need $(1^x, 2^x, 3^x)(4^x) = (1,2,4)(3) = (2,4,1)(3) = (4,1,2)(3)$. The three solutions are

$$\begin{aligned}
&1^x = 1, \quad 2^x = 2, \quad 3^x = 4, \quad 4^x = 3, \quad \text{giving } x = (3,4);\\
&1^x = 2, \quad 2^x = 4, \quad 3^x = 1, \quad 4^x = 3, \quad \text{giving } x = (1,2,4,3);\\
&1^x = 4, \quad 2^x = 1, \quad 3^x = 2, \quad 4^x = 3, \quad \text{giving } x = (1,4,3,2).
\end{aligned}$$