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 7

1. Let G be the cyclic group generated by an element a of order 8.

(*i*) Write down the distinct elements of G. What is the order of G?

(*ii*) Determine the order of each element of G.

(*iii*) Check that, in this group, any two elements that have the same order always generate the same cyclic subgroup.

(*iv*) Which elements of G generate all of G?

(*v*) How many distinct right translates of the set $\{a, a^3, a^5, a^7\}$ are there in G? (List them all.) Are there two distinct translates of this set with elements in common? Is this set a coset of a subgroup?

(*vi*) Repeat the previous part for each of the sets $\{a, a^5\}$, $\{a, a^3, a^5\}$ and $\{a, a^4\}$.

Solution.

(*i*) The distinct elements of G are e (the identity), a, a^2, a^3, a^4, a^5, a^6 and a^7. There are 8 elements: G has order 8.

(*ii*) e has order 1, and a has order 8. To find the order of a^2, compute its successive powers until you get the identity. We find $(a^2)^2 = a^4 \neq e$, $(a^2)^3 = a^6 \neq e$, $(a^2)^4 = a^8 = e$. So a^2 has order 4. Now do a^3 similarly: $a^3 \neq e$, $(a^3)^2 = a^6 \neq e$, $(a^3)^3 = a^9 = a \neq e$, $(a^3)^4 = a^4 \neq e$, $(a^3)^5 = a^7 \neq e$, $(a^3)^6 = a^2 \neq e$, $(a^3)^7 = a^5 \neq e$, $(a^3)^8 = a^8 = e$. So a^3 has order 8. Now a^4: we have $a^4 \neq e$ but $(a^4)^2 = a^8 = e$; so a^4 has order 2. The successive powers of a^5 are a^5, a^2, a^7, a^4, a, a^6, a^3, e. So a^5 has order 8. The successive powers of a^6 are a^6, a^4, a^2, e. So a^6 has order 4. The successive powers of a^7 are a^7, a^6, a^5, a^4, a^3, a^2, a, e. So a^7 has order 8.

(*iii*) From the calculations in Part (*ii*), a^2 and a^6 are the only elements of order 4. The elements of G that are powers of a^2 are e, a^2, a^4 and a^6. The same elements are powers of a^6. So $\langle a^2 \rangle = \langle a^6 \rangle = \{e, a^2, a^4, a^6\}$. We also found that a, a^3, a^5 and a^7 all have order 8. Moreover, for each of these elements we see that the powers of the element yield all the elements of G. So a, a^3, a^5 and a^7 all generate the same subgroup of G: they all generate G itself. There are no other instances of two elements of G having the same order.

(*iv*) The elements that generate G are a, a^3, a^5 and a^7 (see Part (*iii*)).

(*v*) Let $W = \{a, a^3, a^5, a^7\}$. Then $Wa = \{\, wa \mid w \in W \,\} = \{a^2, a^4, a^6, e\}$, and $Wa^2 = \{a^3, a^5, a^7, a\} = W$. Thus $W = We = Wa^2 = Wa^4 = Wa^6$, and $W \neq Wa = Wa^3 = Wa^5 = Wa^7$. There are exactly two distinct right translates of W, and they have no elements in common. The set Wa is a subgroup—it is the cyclic subgroup generated by a^2—and W and Wa are the cosets of this subgroup.

(*vi*) The translates of $\{a, a^5\}$ are itself, $\{a^2, a^6\}$, $\{a^3, a^7\}$ and $\{a^4, e\}$. They are all disjoint from one another, and they are the costs of the subgroup $\{e, a^4\}$. The translates of $\{a, a^3, a^5\}$ are itself, $\{a^2, a^4, a^6\}$, $\{a^3, a^5, a^7\}$, $\{a^4, a^6, e\}$, $\{a^5, a^7, a\}$, $\{a^6, e, a^2\}$, $\{a^7, a, a^3\}$ and $\{e, a^2, a^4\}$. They are not the cosets of a subgroup. It is possible to find two of these translates which have nonempty intersection; indeed, each element of G lies in three distinct translates. Similarly, the set $\{e, a^4\}$ has eight distinct translates: $\{a, a^4\}$, $\{a^2, a^5\}$, $\{a^3, a^6\}$, $\{a^4, a^7\}$, $\{a^5, e\}$. $\{a^6, a\}$, $\{a^7, a^2\}$, $\{e, a^3\}$. Each element of G lies in two of them. They are not the cosets of a subgroup.

2. (*i*) What are the orders of Sym(4), Sym(5), Sym(6), Sym(7) and Sym(8)?

(*ii*) What is the order the group of symmetries of a regular pentagon? Is this group Abelian?

(*iii*) Give an example of a non-Abelian group of order 14.

Solution.

(*i*) If σ is a permutation of $\{1, 2, \ldots, n\}$ then 1^σ, 2^σ, ... , n^σ are the numbers 1, 2, ... , n in some order. There are n possibilities for 1^σ. Once that has been chosen, there are $n-1$ possibilities left for 2^σ, then $n-2$ for 3^σ, and so on. The number of possibilities overall is thus $n(n-1)(n-2)\ldots 3 \cdot 2 \cdot 1 = n!$ (factorial n). So the order of Sym(n) is $n!$. So #Sym(0) = 1, #Sym(1) = 1, #Sym(2) = 2, #Sym(3) = 6, #Sym(4) = 24, #Sym(5) = 120, #Sym(6) = 720, #Sym(7) = 5040 and #Sym(8) = 40320.

(*ii*) A regular pentagon has 10 symmetries. There are 5 rotational symmetries: if $\theta = 2\pi/5$ then the anticlockwise rotations (about the centre) through the angles 0, θ, 2θ, 3θ and 4θ are all symmetries. For each vertex there is a straight line passing through that vertex and the centre, and bisecting the side opposite the vertex. The reflection in this line is a symmetry of the pentagon. There a 5 such lines, and so we get 5 reflection symmetries to go with the 5 rotations, making 10 symmetries altogether. But we should prove that there are no others.

Number the vertices 1 to 5, anticlockwise. Any symmetry must take vertex 1 to one of the other vertices; say vertex i. There are five possibilities for i. Once this has been chosen, vertex 2, being adjacent to 1, must go to one of the two vertices adjacent to i. There are two possibilities. But once this is decided, then there are no further choices: vertex three must go to the vertex that is adjacent to the vertex that 2 goes to and different from the vertex that 0 goes to; and vertex 4 goes to the vertex adjacent to the one vertex 3 goes to and different from the one vertex 2 goes to. And then vertex 5 goes to the only vertex left that nothing else goes to. So the total number of possibilities is just $5 \times 2 = 10$, and these must correspond to the 10 symmetries we described above.

This group is not abelian. The anticlockwise rotation through θ can be represented by the permutation $(1,2,3,4,5)$, and the reflection in the axis if symmetry through vertex 1 can be represented by the permutation $(2,5)(3,4)$. Since

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

we see that there are elements in the group that do not commute with one another.

(*iii*) The group of symmetries of a regular 7-sided polygon has order 14: seven rotations, representable by the powers of $(1,2,3,4,5,6,7)$, and seven reflections, each of which fix one vertex and swap the other three in pairs. One of there reflections corresponds to $(2,7)(3,6)(4,5)$. It is easy to check that this does not commute with $(1,2,3,4,5,6,7)$; so the group is not abelian.

3. The set of all real numbers is a group under addition. Is this group cyclic?

Solution.

It is not cyclic. If it were cyclic, it would have to be generated by some element x. Then the multiples of x would have make up the whole group:

$$\mathbb{R} = \{\,\dots, -x-x-x, -x-x, -x, 0, x, x+x, x+x+x, \dots\,\}.$$

It is clear that there is no such x. Certainly x would have to be nonzero—but then the real number $x/2$ is not a multiple of x.

4. Let H, K be subgroups of a group. Show that the intersection $H \cap K$ satisfies (SG1)–(SG3), and deduce that $H \cap K$ is a subgroup too.
(In words: *the intersection of two subgroups of a group is always a subgroup.*)

Solution.

Let $x, y \in H \cap K$ be arbitrary. Then $x, y \in H$, and since H is a subgroup, and therefore closed under multiplication, it follows that $xy \in H$. But we also have $x, y \in K$, and K is also a subgroup; so $xy \in K$ by the same reasoning. So $xy \in H \cap K$ (since it is in both H and K. But x and y were arbitrary; so we have shown that the product of any pair of elements of $H \cap K$ lies in $H \cap K$. That is, $H \cap K$ satisfies (SG1).

Since H is a subgroup it satisfies (SG2): $e \in H$ (where e is the identity element of G. Since K is a subgroup, $e \in K$ also. So $e \in H \cap K$. Thus $H \cap K$ satisfies (SG2).

Let $x \in H \cap K$ be arbitrary. Then $x \in H$, and since H satisfies (SG3) we must have $x^{-1} \in H$. Similarly, $x \in K$, and hence $x^{-1} \in K$. So $x^{-1} \in H \cap K$, since it is in both H and K. This holds for all $x \in H \cap K$; so (SG3) holds.

Since $H \cap K$ satisfies (SG1), (SG2) and (SG3), by definition it is a subgroup of G.

5. Let G be a group of permutations of the set $\{1, 2, \dots, n\}$, and let H be the set of all elements $\sigma \in G$ that take 1 to 1. That is, $H = \{\,\sigma \in G \mid 1^\sigma = 1\,\}$.

(*i*) By checking (SG1), (SG2) and (SG3), show that H is a subgroup of G.

(*ii*) Suppose that $\tau \in G$ satisfies $1^\tau = 2$.

(a) Show that every element ρ in the coset $H\tau$ satisfies $1^\rho = 2$.

(b) Show that if ρ is any element of G such that $1^\rho = 2$ then $\rho \in H\tau$. (Hint: $\rho = (\rho\tau^{-1})\tau$; show that $\rho\tau^{-1} \in H$.)

Solution.

(*i*) The identity permutation, id, satisfies $i^{\mathrm{id}} = i$ for all $i \in \{1, 2, \dots, n\}$ (by definition). In particular, $1^{\mathrm{id}} = 1$. So $\mathrm{id} \in \{\,\sigma \in G \mid 1^\sigma = 1\,\} = H$. Hence H satisfies (SG2).

Let $\sigma, \tau \in H$. Then $1^\sigma = 1$ and $1^\tau = 1$. But by the definition of permutation multiplication, $1^{\sigma\tau} = (1^\sigma)^\tau$. So

$$1^{\sigma\tau} = (1^\sigma)^\tau = 1^\tau = 1,$$

and so $\sigma\tau \in H$. This holds whenever $\sigma, \tau \in H$; so H is closed under multiplication—that is, it satisfies (SG1).

Let $\sigma \in H$. Then $1 = 1^\sigma$, and so

$$1^{\sigma^{-1}} = (1^\sigma)^{\sigma^{-1}} = 1^{\sigma\sigma^{-1}} = 1^{\mathrm{id}} = 1.$$

So $\sigma^{-1} \in H$, and this holds whenever $\sigma \in H$. So H satisfies (SG3) also. So H is a subgroup.

(*ii*) Let $\rho \in H\tau$. Then $\rho = \sigma\tau$ for some $\sigma \in H$. Since $\sigma \in H$, we have $1^\sigma = 1$, and it follows that

$$1^\rho = 1^{\sigma\tau} = (1^\sigma)^\tau = 1^\tau = 2.$$

Since ρ was an arbitrary element of $H\tau$, we have shown that $1^\rho = 2$ for all $\rho \in H\tau$.

Let $\rho \in G$ satisfy $1^\rho = 2$. Then

$$1^{\rho\tau^{-1}} = (1^\rho)^{\tau^{-1}} = 2^{\tau^{-1}} = (1^\tau)^{\tau^{-1}} = 1^{\tau\tau^{-1}} = 1^{\mathrm{id}} = 1.$$

So $\rho\tau^{-1} \in H$, and so $\rho\tau^{-1}\tau \in H\tau$. That is, $\rho \in H\tau$, as required.