Queen Mary University of London

MTH4104 **Introduction to Algebra**

Week 11 tutorial questions **w/c 4 April 2022**

This sheet contains questions for you to work through in your tutorial, singly or in a group.

It's important to work through lots of questions for practice. Remember that mathematics is not a spectator sport! If you want more questions, look at the "Extra questions" sheets on QMPlus.

Question 1 Let $g = (1\ 5\ 6\ 10\ 4\ 9)(2\ 8\ 11\ 3)$ and $h = (1\ 10\ 3\ 9\ 7\ 6\ 11)(2\ 8)(4\ 5)$ be permutations in S_{11}.

(a) Write g in two-line notation.

(b) Calculate h^{-1}, $g \circ h$, and $h^{-1} \circ g \circ h$[1].

(c) What is the order of g? What is the order of $h^{-1} \circ g \circ h$? Explain how and why these two numbers are related.

Solution (a) The two-line notation for a permutation is its table of values as a function. So just write $1, \ldots, 11$ in the top line, and then underneath each of those, write down the number following it in the cycle notation for g. 7 isn't in the cycle notation, which means $g(7) = 7$. We get

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 5 & 8 & 2 & 9 & 6 & 10 & 7 & 11 & 1 & 4 & 3 \end{pmatrix}.$$

(b) For h^{-1}, just read the cycles backwards:

$$h^{-1} = (11\ 6\ 7\ 9\ 3\ 10\ 1)(8\ 2)(5\ 4).$$

For $g \circ h$, the procedure to compute it directly in the cycle notation is as follows. Open a bracket and put in the first number 1. Then

$$1 \mapsto 10 \text{ (by } h) \ \mapsto 4 \text{ (by } g),$$

so write 4 next in the bracket. Then

$$4 \mapsto 5 \text{ (by } h) \ \mapsto 6 \text{ (by } g),$$

[1] If you want more questions of this type, see `http://www.maths.qmul.ac.uk/fink/PermutationComputations.html`.

so write 6 next in the bracket. Then

$$6 \mapsto 11 \text{ (by } h) \ \mapsto 3 \text{ (by } g),$$

so write 5 next in the bracket. Then

$$3 \mapsto 9 \text{ (by } h) \ \mapsto 1 \text{ (by } g),$$

which completes the cycle

$$(1\ 4\ 6\ 3).$$

We are not yet done with the product. Open another bracket and put in 2, the first number not yet accounted for. Then

$$2 \mapsto 8 \text{ (by } h) \ \mapsto 11 \text{ (by } g),$$

so write 10 next in the bracket. Then

$$11 \mapsto 1 \text{ (by } h) \ \mapsto 5 \text{ (by } g),$$

etcetera. This gives us the cycle

$$(2\ 11\ 5\ 9\ 7\ 10).$$

Finally, 8 is the smallest number unaccounted for, and tracing its images shows that it is a fixed point. We now have all the elements accounted for and conclude

$$gh = (1\ 4\ 6\ 3)(2\ 11\ 5\ 9\ 7\ 10).$$

Adding the (8) is optional.

Of course, it would be also perfectly acceptable to convert g and h into the two-line notation and compose them as usual.

For $h^{-1} \circ g \circ h$, multiply the two permutations just found by the same procedure:

$$h^{-1} \circ g \circ h = (1\ 5\ 3\ 11\ 4\ 7)(2\ 6\ 10\ 8)$$

with optional (9).

(c) The cycle lengths of $h^{-1} \circ g \circ h$ are the same as those of g, namely $6, 4, 1$, and thus they are of the same order, 12.

This equality of orders is a general property of the elements g and $h^{-1} \circ g \circ h$ in any group. We call two such elements *conjugate*; you may have seen this word before in the context of matrix multiplication.

Informally, the reason why g and $h^{-1} \circ g \circ h$ have the same order here is because "$h^{-1}gh$ is just g with the elements of $\{1, \ldots, n\}$ given different names": the "new name" of any number $a \in \{1, \ldots, n\}$ is $h^{-1}(a)$. Indeed,

$$h^{-1} \circ g \circ h(\underline{h^{-1}}(a)) = h^{-1} \circ g \circ h \circ h^{-1}(a) = h^{-1} \circ g(a) = \underline{h^{-1}}(g(a)).$$

Think of the underlined h^{-1} as "renaming", and what this equation says is: "$h^{-1} \circ g \circ h$ applied to a renamed element equals the renamed version of g applied to the original element".

If you wanted to prove this formally for all groups, the key property to establish would be that for any natural number n, we have

$$(h^{-1} \circ g \circ h)^n = h^{-1} g^n h.$$

[Expand it out yourself and see! In fact this is actually true for any integer n, negatives included.] So $(h^{-1} \circ g \circ h)^n$ becomes 1 for the first time at the same exponent n for which $h^{-1} \circ g^n \circ h$ does. But the equation $h^{-1} \circ g^n \circ h = 1$ is equivalent to $g^n = h \circ 1 \circ h^{-1} = 1$, so this first n is also the order of g.

Question 2 Does S_8 contain

(a) a permutation of order 14?

(b) a permutation of order 15?

(c) a permutation of order 16?

Explain why.

Solution This is an exercise with the fact that the order of a permutation is the lcm of the lengths of its cycles. The question is: can we write these numbers 14, 15, 16 as lcms of lists of positive integers, whose sum is at most 8? If the sum is larger than 8, then we can't fit all the cycles into a permutation in S_8.

(b) Yes, it does. We recognise that $15 = \mathrm{lcm}(5,3)$, and we can fit a cycle of length 5 and one of length 3 into a permutation in S_8, such as $(1\ 2\ 3\ 4\ 5)(6\ 7\ 8)$.

(a) We can't use a cycle of length 14 in S_8; that's too long. There's another way to write 14 as an lcm, namely $14 = \mathrm{lcm}(7,2)$, but this still doesn't work, since $7+2 = 9 > 8$ so we can't fit a cycle of length 7 and a cycle of length 2 together. Since these are the only ways to get 14 as an lcm—the factor of 7 has to be somewhere, the factor of 2 has to be somewhere, they're either together or apart—we've exhausted all the ways we might have made a permutation of order 14 without success. The answer is No.

(c) Working out the lcm possibilities for this one might need a little more thought. Remember our rule for computing the lcm using prime factorisations: to find the lcm of a list of natural numbers, we write out each of their prime factorisations, using the same primes in each factorisation, and then for each prime, take the largest exponent appearing on that prime. As I wrote it in symbols, if $a = p_1^{e_1} \cdots p_k^{e_k}$ and $b = p_1^{f_1} \cdots p_k^{f_k}$ then

$$\mathrm{lcm}(a,b) = p_1^{\max(e_1,f_1)} \cdots p_k^{\max(e_k,f_k)},$$

and similarly for more than two primes.

Since $16 = 2^4$, the only way 16 can be an lcm of a list of numbers $a_1, \ldots, a_n$ is if one of those numbers itself, say a_i contains "2^4" in its prime factorisation. But then a_i is a multiple of 16. (A little more thought shows a_i has to *be* 16, i.e. there can't be any other factors; but my proof can get away with not making that observation.) Since a_i is a positive multiple of 16, it is greater than 8, so I can't use it as the length of a cycle in S_8. So the answer is No again.

Question 3 Let the operation $\circ$ be given on a set $G = \{e, a, b, c, d\}$ by the following table.

$\circ$	e	a	b	c	d
e	e	a	b	c	d
a	a	e	d	b	c
b	b	c	e	d	a
c	c	d	a	e	b
d	d	b	c	a	e

Is $(G, \circ)$ a group? Explain.

Solution The putative Cayley table for G has all the easy-to-see properties that a group should have. It has an identity, namely e, since the row and column labelled by e are the same as the header row and column, implying $e \circ x = x = x \circ e$ for every $x \in G$. Also, G appears to satisfy the cancellative property, since every element appears once in each row and column of the table. In particular G satisfies the inverse law. An e appears in each row, giving for each element x an element x^{-1} such that $x \circ x^{-1} = e$. In fact $x^{-1} = x$ in every case so $x^{-1} \circ x = e$ as well: don't forget that cancelling on *both* sides is necessary for an inverse!

However, when we start testing the associative law, we see quickly $(G, \circ)$ does *not* satisfy the associative law and is therefore *not* a group. One counterexample among many is that

$$(a \circ b) \circ c = d \circ c = a$$

is not equal to

$$a \circ (b \circ c) = a \circ d = c.$$

Question 4 Let G be the set of integers with the operation $\circ$ defined by

$$x \circ y = x + y + 1.$$

Prove that $(G, \circ)$ is a group.

Solution We must prove the group axioms.

Closure. We must check that $a \circ b$ is actually an element of G, if a and b are elements of G. This is clear: if a and b are integers, so is $a + b + 1$.

Associativity. We must show that

$$(a \circ b) \circ c = a \circ (b \circ c).$$

The left side is

$$(a \circ b) \circ c = (a + b + 1) \circ c = a + b + 1 + c + 1$$

and the right side is

$$a \circ (b \circ c) = a \circ (b + c + 1) = a + b + c + 1 + 1,$$

which are equal.

Identity. We must find an element $e \in G$ such that $a \circ e = a = e \circ a$ for all $a \in G$. It is easy to see by solving the resulting equation that $e = -1$ works, for then

$$a \circ e = a + (-1) + 1 = a$$

and

$$e \circ a = (-1) + a + 1 = a$$

for any $a \in G$.

Inverses. We must show that for any $a \in G$, there is a $b \in G$ such that $a \circ b = e = b \circ a$, where $e = -1$ is the identity element we found in the previous part. Again, solving the equations that result quickly leads to identifying $b = -a - 2$ as the inverse of a. This works because

$$a \circ b = a + (-a - 2) + 1 = -1 = e$$

and

$$b \circ a = (-a - 2) + a + 1 = -1 = e.$$