Queen Mary University of London

MTH4104 **Introduction to Algebra**

Extra questions for chapter 6 **Spring 2022**

These questions are for you to practice with on your own schedule. You may e.g. want to try some each week as their topics come up in lectures, or use them in exam revision.

6 Permutations

6.1 Definition and notation

Question 6.1.1 Let m be a positive integer. Let a and b be integers such that $\gcd(a,m) = 1$. Prove that the function f defined by

$$f(x) = [a]_m \cdot x + [b]_m$$

is a permutation of the set $\mathbb{Z}_m$.

Solution A permutation on a set X is just a bijection $X \to X$. The given function f is evidently a function from $\mathbb{Z}_m$ to $\mathbb{Z}_m$, so what we have to prove is that it is a bijection. A bijection is a function which is one-to-one and onto, so we must prove each of these properties.

One-to-one. What we must prove is that, if x and y are elements of $\mathbb{Z}_m$ such that $f(x) = f(y)$, then $x = y$. (If the way you learned the definition of one-to-one is the converse of this, that's fine; but your first step would have to be replacing your statement with the converse, or proof by contradiction, bringing you back to my statement.)

So we assume $f(x) = f(y)$, that is

$$[a]_m \cdot x + [b]_m = [a]_m \cdot y + [b]_m.$$

Since $\mathbb{Z}_m$ is a ring, we may use the facts we have proved about rings on this equality. We start with the additive cancellation law to cancel the $+[b]_m$ on both sides: thus our assumption implies

$$[a]_m \cdot x = [a]_m \cdot y.$$

Now, since $\gcd(a,m) = 1$, we know that $[a]_m$ has a multiplicative inverse, and this is exactly what we need to use the multiplicative cancellation law and conclude

$$x = y.$$

This is what we were after; the proof of one-to-one is finished.

Onto. Now we must prove that, for every $y \in \mathbb{Z}_m$, there exists $x \in \mathbb{Z}_m$ so that $f(x) = y$. By definition of f, our objective is

$$[a]_m \cdot x + [b]_m = y.$$

This is a linear equation, and we've discussed how to solve these in a ring. First subtract $[b]_m$ from both sides; then multiply both sides by $[a]_m$, which we know exists as I said above. This gives

$$x = [a]_m^{-1} \cdot (y - [b]_m).$$

Indeed, now

$$\begin{aligned} f(x) &= f([a]_m^{-1} \cdot (y - [b]_m)) \\ &= [a]_m \cdot [a]_m^{-1} \cdot (y - [b]_m) + [b]_m \\ &= (y - [b]_m) + [b]_m \\ &= y. \end{aligned}$$

So we have found the requisite x and proved that f is onto.

This completes the proof that f is a bijection, and therefore a permutation of $\mathbb{Z}_m$.

6.2 Composition

Question 6.2.1 Let X and Y be finite sets, and $f : X \to Y$ be a function. In lecture I asserted that f has an inverse function if and only if it is a bijection. This is a corollary of the following:

(a) Prove that there exists a function g such that $f \circ g$ is the identity function on Y if and only if f is a surjection.

(b) Prove that there exists a function h such that $h \circ f$ is the identity function on X if and only if f is an injection.

(c) Prove that, if f is a bijection, then the g and h from parts (a) and (b) can be chosen to be equal to each other.

Solution (a) Suppose that $(f \circ g)(y) = y$ for all $y \in Y$. Then for all $y \in Y$, there is an $x \in X$ such that $f(x) = y$: indeed, $x = g(y)$ works, because $f(g(y)) = y$ by assumption. So f is surjective.

Conversely, suppose f is a surjection. Then we can define g as follows: for each $y \in Y$, pick any one of the elements $x \in X$ such that $f(x) = y$, and let $g(y) = x$. Clearly this definition ensures that $f(g(y)) = y$ for each $y \in Y$.

(b) Suppose that $(h \circ f)(x) = x$ for all $x \in X$. Let x_1 and x_2 be different elements of x; we wish to show that $f(x_1)$ and $f(x_2)$ are also different. But if they weren't, we would have

$$x_1 = h(f(x_1)) = h(f(x_2)) = x_2,$$

contradicting that x_1 and x_2 were chosen to be different. So f is injective.

Conversely, suppose f is an injection. Then we can define h as follows. For $y \in Y$, if $y = f(x)$ for some x, then this x is unique; let $h(y) = x$. Otherwise, if y is not in the range of f, let $h(y)$ take any arbitrary value. Clearly this definition ensures that $h(f(x)) = x$ for each $x \in X$.

(c) This is an immediate consequence of our constructions of g and h. If f is a bijection, then both g and h are the function that is completely defined by saying that it maps $f(x)$ back to x for each x. So g and h are equal. (Despite the wording of the question, there is not actually any choice in what g or h is in this situation.)

Commentary. The finiteness assumption is not necessary for this question. I put it there for two reasons. The more prosaic reason is because finite sets are easier to think about, play with, and try examples of.

Here's the other reason. If the sets were infinite, then the way I constructed g in part (a) would rely on the *axiom of choice*, which says that, given an infinite family of sets, you can choose an element arbitrarily from each one. As innocuous as this axiom may seem, it is actually independent of the remaining axioms of standard (Zermelo-Fraenkel) set theory, i.e. you cannot prove it from the remaining axioms! Zermelo introduced the axiom of choice in 1904, and for the better part of the twentieth century it was controversial, with many set theorists not accepting it. Nowadays it is generally accepted. All the same, given my devotion to the axiomatic method, it didn't feel right to ask you to construct a function in a way that isn't actually allowed under a historically popular set of axioms for set theory.

Question 6.2.2 Let R be a relation on the set $\{1,\ldots,n\}$. Let us say that a permutation $f \in S_n$ is a *symmetry* of R if and only if

$$\{(f(x), f(y)) : (x,y) \in R\} = R.$$

Prove that:

(a) The identity permutation e is a symmetry of R.

(b) If f is a symmetry of R, then so is f^{-1}.

(c) If f and g are symmetries of R, then so is $f \circ g$.

Solution Once we introduce groups, we'll see that the properties listed above are enough to show that the set of symmetries of R is a group. That's why I put this question here, to prove at least one case of my claim that groups are useful for studying symmetry.

You might object that my notion of symmetry is strange. But there are connections with the geometric meaning of symmetry. Question 1 on the week 12 coursework is an example: if I have a "regular enough" geometric figure, like the regular pentagon in that question, I can make a relation on the set of corners of the figure:

$$R = \{(c_1, c_2) : c_1 \text{ and } c_2 \text{ are directly connected by an edge}\}.$$

Then the symmetries of this relation will be the same permutations that describe symmetries of my figure.

Enough chat, onto the proof. This is a proof where we'll have to be very very careful about set-builder notation, so make sure you're on top of that notation before reading on!

(a) By definition, the identity permutation of e is a symmetry of R if and only if

$$\{(e(x),e(y)) : (x,y) \in R\} = R.$$

But $(e(x),e(y)) = (x,y)$, so the set on the left hand side is

$$\{(x,y) : (x,y) \in R\},$$

which is indeed the same as R.

(b) We assume that f is a symmetry of R, which means

$$\{(f(x),f(y)) : (x,y) \in R\} = R. \tag{1}$$

We must show the corresponding statement for f^{-1}, namely,

$$\{(f^{-1}(a),f^{-1}(b)) : (a,b) \in R\} = R.$$

I've used different letters in place of x and y just to make it harder to confuse my assumption with my goal[1].

How can we do this? For want of better, let's start by using the definition of f^{-1}, since that is often a good place to start. $f^{-1}(a)$ is the element $c \in \{1,\ldots,n\}$ such that $f(c) = a$. Similarly, $f^{-1}(b) = d$ for the element d such that $f(d) = b$. Therefore, the equality that we are trying to prove can be rewritten as

$$\{(c,d) : f(c) = a, f(d) = b, (a,b) \in R\} = R,$$

or, cleaning up the needless letters,

$$\{(c,d) : (f(c),f(d)) \in R\} = R. \tag{2}$$

Is that progress? Maybe. Anyway, there's another idea we can generate without needing cleverness. We have to prove two sets equal, and there's a roadmap for proving two sets equal. Namely, we take an element of each set, and show it is an element of the other. Let's do that.

Assume (c,d) is an element of the set on the left hand side of equation (2). This means $(f(c),f(d)) \in R$. Using the assumption that f is a symmetry of R, equation (1), we can say

$$(f(c),f(d)) \in \{(f(x),f(y)) : (x,y) \in R\}.$$

But since f is an injection, the only way to make $(f(c),f(d))$ look like $(f(x),f(y))$ is to take $c = x$ and $d = y$. This means that $(c,d) \in R$, which is what we wanted!

The other inclusion is quicker. We assume that $(a,b) \in R$, and want to show

$$(a,b) \in \{(c,d) : (f(c),f(d)) \in R\}.$$

[1] That is, to make it easier to mind my ps and qs!

In other words, we want to show $(f(a), f(b)) \in R$. But $(a,b) \in R$ implies that $(f(a), f(b))$ is in the set on the left side of equation (1), and thus it's also in the set on the right hand side, namely R. Done!

(c) We assume that f and g are symmetries of R, which means

$$\{(f(x), f(y)) : (x,y) \in R\} = R \qquad \text{and}$$
$$\{(g(x), g(y)) : (x,y) \in R\} = R.$$

We want to show that $f \circ g$ has the same property,

$$\{\big(f(g(x)), f(g(y))\big) : (x,y) \in R\} = R.$$

Our roadmap for proving two sets equal is to prove that each set is a subset of the other. Let's start with the $\subseteq$ containment. Let $(x,y) \in R$. Is the pair $\big(f(g(x)), f(g(y))\big)$ an element of R? Our assumption about g implies that $\big(g(x), g(y)\big) \in R$. Now we can substitute $g(x)$ and $g(y)$ for x and y our assumption about f, and this assumption now proves that $\big(f(g(x)), f(g(y))\big) \in R$.

Now for the $\supseteq$ containment. For this containment, we start with an element $(a,b) \in R$, and want to write $(a,b) = \big(f(g(x)), f(g(y))\big)$ for some $(x,y) \in R$ in order to prove (a,b) is in the set on the left hand side. Our assumption about f implies that $(a,b) = \big(f(c), f(d)\big)$ for some $(c,d) \in R$. And our assumption about g implies that $(c,d) = \big(g(x), g(y)\big)$ for some $(x,y) \in R$. If two tuples are equal then corresponding components are equal, so $c = g(x)$ and $d = g(y)$, and substituting these into the first equality gives $(a,b) = \big(f(g(x)), f(g(y))\big)$ where still $(x,y) \in R$. This completes the proof of part (c).

6.3 Cycles

Question 6.3.1

(a) Convert the element $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 1 & 7 & 2 & 3 & 9 & 5 & 8 & 4 \end{pmatrix}$ of S_9 from two-line notation to cycle notation.

(b) Convert the element $g = (1\ 10\ 4\ 6)(5\ 8)(7\ 9\ 3)$ of S_{10} from cycle notation to two-line notation[2].

Solution (a) Let's use the algorithm from the lecture notes. Start with the first element, 1. Follow its successive images under f until it returns to its starting point:

$$f : 1 \mapsto 6 \mapsto 9 \mapsto 4 \mapsto 2 \mapsto 1.$$

This gives us a cycle $(1\ 6\ 9\ 4\ 2)$.

Since this cycle does not contain all the elements of the set $\{1, \ldots, 9\}$, we're not done. We choose the smallest unused element, which is 3, and repeat the procedure:

$$f : 3 \mapsto 7 \mapsto 5 \mapsto 3,$$

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

so we have a cycle $(3\ 7\ 5)$ disjoint from the first.

We are still not finished, since we have not seen the element 8 yet. In this case $f : 8 \mapsto 8$, so (8) is a cycle with a single element. Now we have seen all elements of $\{1,\ldots,9\}$, and have the cycle decomposition

$$f = (1\ 6\ 9\ 4\ 2)(3\ 7\ 5)(8) = (1\ 6\ 9\ 4\ 2)(3\ 7\ 5).$$

We can write in the (8) or not; either way is correct. We could have also reordered the cycles, or started them at different points. I did it this way just to be systematic.

(b) This is done simply by writing $1,\ldots,10$ in the top line, then finding each integer $1,\ldots,10$ in the cycle notation for g and recording underneath the next number in that cycle. We get

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

Bear in mind that the next number in a cycle after the last one is the first one, and that a number that doesn't appear (in this case 2) is in a cycle of length one so satisfies $g(2) = 2$.

Question 6.3.2

(a) Let f be a permutation which is a single cycle of length m. Prove that if m is odd, then $f \circ f$ is also a single cycle of length m, and if m is even, then $f \circ f$ decomposes into two disjoint cycles of length $m/2$.

(b) Let $g \in S_n$ be a permutation. Describe a method for answering the following question: does there exist a permutation $f \in S_n$ such that $f \circ f = g$?

Solution (a) Let's give the names $x_1,\ldots,x_m$ to the elements in the cycle, so that $f = (x_1\ x_2\ \ldots\ x_m)$. In other words, for all $i = 1,\ldots,m$,

$$f(x_i) = \begin{cases} x_{i+1} & \text{if } i \leq m-1 \\ x_1 & \text{if } i = m. \end{cases}$$

When we apply this formula twice to work out $(f \circ f)(x_i) = f(f(x_i))$, there are three cases. Either $x_i = x_m$, or $f(x_i) = x_m$, or neither of these are true:

$$f(f(x_i)) = \begin{cases} f(x_{i+1}) & \text{if } i \leq m-1 \\ f(x_1) & \text{if } i = m \end{cases} = \begin{cases} x_{i+2} & \text{if } i \leq m-2 \\ x_1 & \text{if } i = m-1 \\ x_2 & \text{if } i = m. \end{cases}$$

This looks a little bit tidier rewritten as

$$f(f(x_i)) = \begin{cases} x_{i+2} & \text{if } i \leq m-2 \\ x_{i-m+2} & \text{if } i > m-2. \end{cases}$$

Don't be scared of this. It's just a way of writing down that $f \circ f$ "advances two steps along" the cycle f.

Now let's put that back in cycle notation. Following the algorithm, we start writing out the first cycle in $f \circ f$ as

$$(x_1\ x_3\ x_5\ \ldots)$$

When does this cycle end? This is where the parity of m matters. If m is odd, then we reach x_m, which is mapped to x_2, and we continue with even xs. The cycle finally closes at

$$f \circ f = (x_1\ x_3\ \ldots\ x_m\ x_2\ x_4\ \ldots\ x_{m-1}).$$

This cycle contains all the elements that were in f, i.e. its length is also m.

But if m is even, then our cycle starting with odd xs never reaches x_m. Instead we get to x_{m-1}, and then $f(f(x_{m-1})) = x_1$ so that cycle closes, and we must start another at x_2. After the second cycle finishes we have

$$f \circ f = (x_1\ x_3\ \ldots\ x_{m-1})(x_2\ x_4\ \ldots\ x_m).$$

Now all the elements are exhausted, and as you can see we have two cycles, each containing half of the elements that were in the cycle f, so length $m/2$ each.

(b) Just as we argued in Proposition 6.4, if $f = c_1 \circ \cdots \circ c_k$ is a composition of disjoint cycles c_1 through c_k, then $f \circ f$ can be worked out by doing each cycle twice individually, and the cycles don't interact with each other. That is,

$$f \circ f = (c_1 \circ c_1) \circ \cdots \circ (c_k \circ c_k).$$

(You may see how this is really a claim about certain permutations that *commute*.)

In part (a) we worked out what each of these $c_i \circ c_i$ can be. Each one is either an odd cycle, or two disjoint cycles of the same length. And if the c_i are disjoint, so are the $c_i \circ c_i$, because $c_i \circ c_i$ moves the same elements as c_i does.

So if we hope to write a given permutation $g \in S_n$ as $f \circ f$, what we need to do is write g in cycle notation, and then allocate its cycles to the various pieces $c_i \circ c_i$ in $f \circ f$. Let's say $g = d_1 \circ \cdots \circ d_\ell$, where the d_i are disjoint cycles. If d_i has odd length, then d_i can be $c_i \circ c_i$ all by itself. But if d_i has even length we can't do that, and instead we have to find another d_j (with $j \neq i$) of the same length, and pair them off as a $c_i \circ c_i$ together.

Running through this logic for all the d_i, we conclude that there exists $f \in S_n$ such that $g = f \circ f$ if and only if

for every even number $2k$, the number of cycles in g of length $2k$ is even.