MA10209 Algebra

Sheet 2 solutions: GCS

Course website http://people.bath.ac.uk/masgcs/diary.html

Hand in work to your tutor at the time specified by your tutor. The latest possible hand in time is be 17:15, Monday Oct 15 because after that I will put up model solutions at the website. On twitter I am `@GeoffBath` *and my email address is* `G.C.Smith@bath.ac.uk`.

1. In each case, determine whether the statement really defines a map, or it is defective in some way.

   (a) $f : \mathbb{C} \longrightarrow \mathbb{C}$ defined by $f(z) = 1/z$ for each $z \in \mathbb{C}$.
   Solution This is not a map because $f(0)$ is not assigned a value. You could rectify this by making 0 an exception, and defining $f(0)$ as you please.

   (b) $g : \mathbb{C} \longrightarrow \mathbb{C}$ defined, for each $z \in \mathbb{C}$, by letting $g(z)$ be the complex number such that $g(z)^2 = z$.
   Solution This is not a map because the alleged recipe is ambiguous. For example $i^2 = (-i)^2 = -1$, so $g(-1)$ is not properly defined.

   (c) h is the function $\cos x$.
   Solution This is not a map because neither domain nor codomain is specified.

   (d) $j : \mathbb{R} \longrightarrow \mathbb{R}$ defined, for each $x \in \mathbb{R}$, by $j(x) = \sin(\cos(\tan(x)))$.
   Solution This is not a map because $\tan \pi/2$ is not a real number.

   (e) $k : \mathbb{Q} \longrightarrow \mathbb{Q}$ by, for each $x \in \mathbb{Q}$, $k(x) = \sqrt{|x|}$ (with the convention that $\sqrt{}$ means take the non-negative square root).
   Solution This is not a map because $\sqrt{2} \notin \mathbb{Q}$.

2. In each case, determine which of the properties *injectivity*, *surjectivity* and *bijectivity* are enjoyed by the given function. Please give reasons.

   (a) $f_1 : \mathbb{N} \longrightarrow \mathbb{Z}$ defined by $f_1(x) = x^2$ for each $x \in \mathbb{N}$.
   Solution This map is injective because if $m, n \in \mathbb{N}$ and $f_1(m) = f_1(n)$, then $m^2 = n^2$ so $(m - n)(m + n) = 0$ and so $m = n$. It is not surjective since -1 is not a square of a natural number. Since this map is not surjective, it is also not bijective.

   (b) $f_2 : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $f_2(x) = x^2$ for each $x \in \mathbb{Z}$.
   Solution This map is neither injective nor surjective. It is not injective because $1^2 = (-1)^2$. It is not surjective because -1 is not a square of an integer. This miserable map is therefore not bijective.

   (c) $f_3 : \mathbb{C} \longrightarrow \mathbb{R}$ defined by $f_3(x) = |x|$ for each $x \in \mathbb{C}$.
   Solution This map is not injective since $f_3(1) = f_3(-1)$. It is not surjective since $|x|$ is never negative. Therefore f_3 is not bijective.

(d) $f_4 : \mathbb{C} \longrightarrow \{r^2 \mid r \in \mathbb{R}\}$ defined by $f_4(x) = |x|$ for each $x \in \mathbb{C}$.
Solution It is not injective because $1^2 = (-1)^2$. However, it is surjective because if $y \in \{r^2 \mid r \in \mathbb{R}\}$, then $f_4(y) = y$. This map is therefore not bijective.

(e) $f_5 : \mathbb{N} \longrightarrow \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ defined by letting $f_5(x)$ be the leftmost digit in the ordinary base 10 (decimal) representation of n.
Solution This map is not injective because $f_5(1) = 1 = f_5(10)$. However, it is surjective because if $z \in \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, then $f_5(z) = z$. This map is therefore not bijective.

(f) $f_6 : \{r \mid r \in \mathbb{R}, -\pi/2 < r < \pi/2\} \longrightarrow \mathbb{R}$ defined by letting $f_6(x) = \tan x$.
Solution The map tan is well-defined on this interval (dodgy places such as $\pm\pi/2$ are not in the domain), and is strictly increasing. It is therefore injective. Also between $-\pi/2$ and $\pi/2$, tan assumes all real values. This function is therefore surjective and hence bijective.

3. Let $I_n = \{1, 2, \ldots n\}$ be the set which consists of the first n natural numbers, and let $S = \{0, 1\}$. In each case you should justify your answer, for a numerical response will not suffice.

(a) How many maps f are there such that $f : I_n \longrightarrow S$?
Solution You can define a map by a finite sequence of n independent choices: $f(1)$ can be 0 or 1, then $f(2)$ can be 0 or 1 and so on. There are 2^n such sequences of choices, and so 2^n such maps. It is no accident that the choices, viewed as lists of digits, are the numbers from 0 to $2^n - 1$ written in binary, with initial strings of zeros as padding on the front to make the string have length n.

(b) How many surjective maps f are there such that $f : I_n \longrightarrow S$?
Solution There are 2^n maps from I_n to S, of which two, the constant maps, are not surjective. Therefore there are $2^n - 2$ surjective maps.

(c) How many injective maps f are there such that $f : I_n \longrightarrow S$?
Solution If $n > 2$ there are none. If $n = 2$ there are two injective maps (the bijective maps). If $n = 1$ there are two injective maps.

(d) How many bijective maps f are there such that $f : I_n \longrightarrow I_n$?
Solution There are n choices as to the value of $f(1)$. Having defined $f(1)$, there are $n - 1$ choices for the value of $f(2)$ and so on. The total number of bijections is therefore $n!$.

(e) How many surjective maps f are there such that $f : I_n \longrightarrow I_n$?
Solution A surjective map from a set of size n to a set of size n must also be injective, and therefore bijective. Conversely, any such bijective map must be surjective. Therefore this question is simply a repetition of the previous question, so the answer is $n!$

(f) How many injective maps f are there such that $f : I_n \longrightarrow I_n$?
Solution An injective map from a set of size n to a set of size n must also be surjective, and therefore bijective. Conversely, any such bijective map must be injective. Therefore this question is simply a repetition of the previous question, so the answer is $n!$

4. Let $f : A \longrightarrow B$ be a map. Let $X = \{f(a) \mid a \in A\} \subseteq B$. Show that there is a (natural) surjective map $g : A \longrightarrow X$ and a (natural) injective map $h : X \longrightarrow B$ such that $f = h \circ g$. *Hint: There are obvious recipes which define the maps g and h. This is what the word 'natural' means in this context.*
Solution Define g by $g(a) = f(a)$ for each $a \in A$. This is clearly surjective. Define $h : X \longrightarrow B$ by $h(x) = x$ for every $x \in X$. This is clearly injective. Moreover, if $a \in A$, then $(h \circ g)(a) = h(g(a)) = h(f(a)) = f(a)$. Now $h \circ g$ and f have the same domain, the same codomain, and act the same way, so $h \circ g = f$. *This is an interesting factorization result: any map can be expressed as a surjective map composed with an injective map; surjective first, injective last.*

5. Suppose that $f : A \longrightarrow B$ and $g : B \longrightarrow C$ are maps. *In each case, you should either give a proof that the result follows, or a specific example to show that it does not follow.*

   (a) Suppose that $g \circ f$ is injective. Does it follow that f is injective?
   Solution Yes it does follow that f is be injective. This is because if $a_1, a_2 \in A$ and $f(a_1) = f(a_2)$, then $g(f(a_1)) = g(f(a_2))$ and so $(g \circ f)(a_1) = (g \circ f)(a_2)$. However, $g \circ f$ is injective so $a_1 = a_2$.

   (b) Suppose that $g \circ f$ is injective. Does it follow that g is injective?
   Solution It does not follow. Let $A = \{1\}, B = \{1, 2\}$ and $C = A$. Define f by $f(1) = 1$, and g by $g(1) = 1$ and $g(2) = 1$. Therefore g is not injective but $g \circ f : \{1\} \longrightarrow \{1\}$ is defined by $(g \circ f)(1) = 1$ and is injective.

   (c) Suppose that $g \circ f$ is surjective. Does it follow that f is surjective?
   Solution It does not follow. Let $A = \{1\}, B = \{1, 2\}$ and $C = A$. Define f by $f(1) = 1$, and g by $g(1) = 1$ and $g(2) = 1$. Therefore f is not surjective but $g \circ f : \{1\} \longrightarrow \{1\}$ is defined by $(g \circ f)(1) = 1$ and is surjective.

   (d) Suppose that $g \circ f$ is surjective. Does it follow that g is surjective?
   Solution Yes it does follow that g must be surjective. Suppose that $c \in C$. Now $g \circ f$ is surjective so there is $a \in A$ such that $(g \circ f)(a) = c$. Therefore $g(f(a)) = c$. Now $f(a) \in B$ and has the property that $g(f(a)) = c$. Therefore g is surjective.

6. Suppose that $f : A \longrightarrow A$ and $g : A \longrightarrow A$. *In each case, you should either give a proof that the result follows, or a specific example to show that it does not follow.* We omit brackets from compositions of three (or more) functions since the associative law has been established.

   (a) Suppose that $g \circ f$ and $f \circ g$ are both bijective. Does it follow that f and g are both bijective?
   Solution By 5(a) both f and g are injective. By 5(d) both f and g are surjective. Therefore both f and g are bijective.

   (b) Suppose that $f \circ f$ is bijective. Does it follow that f is bijective?
   Solution By 5(a) f is injective. By 5(d) f is surjective, Therefore f is bijective. Alternatively use 6(a) and put $g = f$.

   (c) Suppose that $f \circ g \circ f$ is bijective. Does it follow that g is bijective?
   Solution $f \circ g \circ f = (f \circ g) \circ f$ so by 5(a), f is injective. Also $f \circ g \circ f = f \circ (g \circ f)$,

so by 5(d) f is surjective. Therefore f is bijective and has an inverse map f^{-1}. Now $f^{-1} \circ (f \circ g \circ f)$ is the composition of bijective maps and so is bijective. However $f^{-1} \circ (f \circ g \circ f) = (f^{-1} \circ f) \circ (g \circ f) = \mathrm{Id}_A \circ (g \circ f) = g \circ f$ is bijective. Now $(g \circ f) \circ f^{-1} = g \circ (f \circ f^{-1}) = g \circ \mathrm{Id}_A = g$ is the composition of bijective maps and so is bijective.

7. Consider the maps $f, g : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $f(x) = x + 1$ for each $x \in \mathbb{Z}$ and $g(x) = 2x$ for each $x \in \mathbb{Z}$.

   (a) Determine all maps $h : \mathbb{Z} \longrightarrow \mathbb{Z}$ such that $f \circ h = h \circ f$.
   Solution Suppose that h is such a map. Then $h(x) + 1 = h(x + 1)$ for each integer x $(\star)$. Let $h(0) = t$ for some $t \in \mathbb{N}$. We claim that $h(y) = t + y$ for every $y \in \mathbb{Z}$.

   We will prove this by induction on y when $y \in \mathbb{N}$. Suppose that the result is true when $y = r$ and try to deduce that the result holds when $y = r + 1$. Now $h(r + 1) = h(r) + 1$ by $(\star)$. By inductive hypothesis, $h(r) = t + r$ so $h(r+1) = h(r)+1 = (t+r)+1 = t+(r+1)$. This is precisely what is required, so $h(y) = t + y$ for all natural numbers y.

   Now suppose that $y < 0$. Let $z = -y$. We will prove by induction on $z \in \mathbb{N}$ that $h(-z) = t - z$. This result holds when $z = 0$. Suppose that the result holds when $z = r$, and try to deduce that the result holds when $z = r+1$. Now $h(-r) = h(-r-1)+1$ by $(\star)$. Therefore $h(-r-1) = h(-r)-1$. Now $h(-r) = t - r$ by inductive hypothesis. Therefore $h(-r-1) = (t-r)-1 = t-(r+1)$. This is precisely what is required, so $h(-y) = t - y$ for all natural numbers y.

   Since $h(0) = t$, it follows that $h(x) = t + x$ for all integers x.

   We have not finished, because all we have done is to show that if h commutes (in the sense of composition) with f, then h must be one of these maps given by the recipe $h(x) = t+x$ where t is fixed, and x is arbitrary. We have to check to see if any of the maps of this form actually do commute with f. Suppose that t is an integer and that $h(x) = t+x$ for all $x \in \mathbb{Z}$. We need to compare $f \circ h$ and $h \circ f$. They both have domain $\mathbb{Z}$ and codomain $\mathbb{Z}$, so the action is the only thing at issue. Suppose that $w \in \mathbb{Z}$. Then $(f \circ h)(w) = f(h(w)) = f(t+w) = t+w+1$. On the other hand $(h \circ f)(w) = h(f(w)) = h(w + 1) = t + w + 1$. Therefore $f \circ h = h \circ f$ and all maps of the given form commute with f. Note, by the way, that all these maps h are bijections, something which was not specified in advance.

   (b) Determine all maps $j : \mathbb{Z} \longrightarrow \mathbb{Z}$ such that $g \circ j = j \circ g$.
   Solution A map $j : \mathbb{Z} \longrightarrow \mathbb{Z}$ satisfies our condition if, and only if, $g(j(x)) = j(g(x))$ i.e. $2j(x) = j(2x)$ for each $x \in \mathbb{Z}$. We can manufacture functions which obey this condition readily: for odd m we assign the value of $j(m)$ arbitrarily (i.e. just select an integer value, and you can choose different values for different odd m). The value 0 is special, since $2j(0) = j(0)$ so $j(0) = 0$. If n is even but not 0, define $j(n)$ to be $2j(n/2)$. This is an inductive definition, since if $n/2$ happens to be even, the definition requires $j(n/2)$ to be $2j(n/4)$ and so on. Any map we make in this way will satisfy the condition, and so will commute with g.

(c) Determine all maps $k : \mathbb{Z} \longrightarrow \mathbb{Z}$ such that both $f \circ k = k \circ f$ and $g \circ k = k \circ g$.
Solution We are looking for functions k which arise as solutions to both previous parts. Thus there must be an integer t such that $k(x) = t + x$ for each $x \in \mathbb{Z}$ by part (a). Now from part (b), $k(0) = 0$ so $t = 0$. We need look no further. There is only one possibility; k is the identity function. Now $\mathrm{Id}_{\mathbb{Z}}$ does commute with f and g, and in fact it (composition) commutes with all maps from $\mathbb{Z}$ to $\mathbb{Z}$.

8. Exhibit (i.e. give examples of) bijections between the given sets:

(a) Domain $\mathbb{N}$, codomain $\mathbb{Z}$.
Solution We define such a map $f : \mathbb{N} \longrightarrow \mathbb{Z}$. If n is even, let $f(n) = n/2$. If n is odd, then $f(n) = (1 - n)/2$.

(b) Domain $\mathbb{N}^2$, codomain $\mathbb{Z}$.
Solution Let $X = \{2^u 3^v \mid u, v \in \mathbb{N}\} \subseteq \mathbb{N}$. Define a map $g : \mathbb{N}^2 \longrightarrow X$ by $g((u, v)) = 2^u 3^v$ for all $(u, v) \in \mathbb{N}^2$. Now g is surjective by design. It is also injective because if $2^{u_1} 3^{v_1} = 2^{u_2} 3^{v_2}$ then $2^{u_1 - u_2} = 3^{v_2 - v_1}$. Therefore $u_1 = u_2$ and $v_1 = v_2$ as required.

Define a map $h : X \longrightarrow \mathbb{N}$ as follows. List the elements of X in ascending order of size as $x_1, x_2, x_3, \ldots$. Let $h(x_i) = i$. This is clearly a bijection. Now $h \circ g : \mathbb{N}^2 \longrightarrow \mathbb{N}$ is a composition of bijections and so is a bijection. If we now borrow the map f from part (a), we find that $f \circ (h \circ g) : \mathbb{N}^2 \longrightarrow \mathbb{Z}$ is a composition of bijections and so is a bijection as required.

(c) Domain $\{r \mid r \in \mathbb{R}, 0 < r < 1\}$, codomain $\mathbb{R}$.
Solution Define a map $g : \{r \mid r \in \mathbb{R}, 0 < r < 1\} \longrightarrow \{r \mid r \in \mathbb{R}, -\pi/2 < r < \pi/2\}$ via $g(t) = \pi t - \pi/2$. We must verify that this is a bijection (at some point we you will be able to regard this as obvious, but at the moment we are still being scrupulous). In terms of the number line, multiplication by π is a an enlargement from 0. Then subtraction of $\pi/2$ is a translation. The interval $\{r \mid r \in \mathbb{R}, 0 < r < 1\}$ is thus stretched to have the correct length by holding its (non-existent) left end still, and pulling its (non-existent) right end to the right until the interval has length π. The resulting interval is then slid to the left. We must express this more formally. We have a map from $\{r \mid r \in \mathbb{R}, 0 < r < 1\}$ to $\{r \mid r \in \mathbb{R}, 0 < r < \pi\}$ defined by multiplication by π. There is also a map from $\{r \mid r \in \mathbb{R}, 0 < r < \pi\}$ to $\{r \mid r \in \mathbb{R}, -\pi/2 < r < \pi/2\}$ defined by subtraction of $\pi/2$. Perhaps the recipes which define these two maps are so easy that we will allow ourselves to say that they are each *obviously* bijections. Their composition is therefore a bijection as required.

Now borrow the map f_6 from 2(f), and form the composition of bijections $f_6 \circ g : \{r \mid r \in \mathbb{R}, 0 < r < 1\} \longrightarrow \mathbb{R}$, which must be a bijection.

(d) (interesting) Domain $\{A \mid A \subseteq \mathbb{N}, |A| < \infty\}$, codomain $\mathbb{N}$.
Solution Let $S = \{A \mid A \subseteq \mathbb{N}, |A| < \infty\}$. Define a map $\theta : S \longrightarrow \mathbb{N}$ as follows. $\theta(\emptyset) = 1$ and if $s \in S$ and $s \neq \emptyset$, then $\theta(s) = 1 + \sum_{x \in s} 2^{x-1}$. We prove injectivity: if $\theta(s_1) = \theta(s_2)$, then $\sum_{x \in s_1} 2^{x-1} = \sum_{y \in s_2} 2^{y-1}$, so by uniqueness of binary representations, $s_1 = s_2$. Moreover, θ is surjective, since if $n \in \mathbb{N}$ and $n - 1$ has binary representation $n - 1 = \sum_{x \in T} 2^{x-1}$ for some finite subset T of $\mathbb{N}$, then $\theta(T) = n$. To help understand θ, let us calculate some of its values.

$\theta(\emptyset) = 1$, $\theta(\{1\}) = 1 + 2^0 = 2$, $\theta(\{2\}) = 1 + 2^1 = 3$, $\theta(\{1,2\}) = 1 + 2^0 + 2^1 = 4$, $\theta(\{3\}) = 1 + 2^2 = 5$, $\theta(\{1,3\}) = 1 + 2^0 + 2^2 = 6$, $\theta(\{2,3\}) = 1 + 2^1 + 2^2 = 7$, $\theta(\{1,2,3\}) = 1 + 2^0 + 2^1 + 2^2 = 8$, $\theta(\{4\}) = 1 + 2^3 = 9$, etc

9. (A little trickier) Suppose that S is a finite set of size n and that $f : S \longrightarrow S$ is a bijection. Define $f^0 = \mathrm{Id}_S$ and if $m > 0$ is a positive integer, then we define f^m to be $f \circ f^{m-1}$. Prove that $f^{n!} = \mathrm{Id}_S$, the identity map from S to S.
Solution If $S = \emptyset$ the result is clear so we may assume that $S \neq \emptyset$. Suppose that $s \in S$. Consider the $n+1$ terms $s, f(s), f^2(s), \ldots, f^n(s)$. We introduce the notation $f^0(s)$ for s. Since there are only n elements of S, two of these terms must coincide (they must be the same). Therefore there are integers u, v with $0 \leq u < v \leq n$ such that $f^u(s) = f^v(s)$. Now f is a bijection with inverse f^{-1}. Apply the map $(f^{-1})^u$ to both sides, to discover that $s = f^{v-u}(s)$. Now $0 < v - u = k \leq n$. Therefore there is a positive integer k with $k \leq n$ and $f^k(s) = s$. Now k is a divisor of $n!$ since it appears in the list $1, 2, 3, \ldots, n$. Therefore $n! = kl$ for some positive integer l. Now

$$f^{n!}(s) = f^{kl}(s) = (f^k \circ f^k \circ \cdots \circ f^k)(s)$$

where there are l maps of the form f^k being composed. Now $f^k(s) = s$ so $f^{n!}(s) = s$. Since $s \in S$ was arbitrary, this forces $f = \mathrm{Id}_S$.

10. (Challenge!) This problem concerns polynomials in X with real coefficients. Let $f(X) = 2017X + 1$. Suppose that $g(X)$ and $h(X)$ are polynomials such that $f(g(X)) = g(f(X))$ and $f(h(X)) = h(f(X))$. Prove that $g(h(X)) = h(g(X))$.
Solution Let $k = 2017$, and $c = -1/2016$ be the unique fixed point of f (i.e. $f(c) = c$).

First we study g. Now $g(c) = g(f(c)) = f(g(c))$ so $g(c) = c$. Therefore $g = (X - c)q + c$ where q (or $q(X)$) is a real polynomial. Now $f(g(X)) = g(f(X))$ and we can write f as $k(X - c) + c$. Therefore

$$k(X - c)q + c = k(X - c)q(f(X)) + c$$

and so $q(X) = q(f(X)) = q(f(f(X))) = q(f(f(f(X))))$ etc. We have repeatedly replaced X by $f(X)$ in the polynomial equation $q(X) = q(f(X))$. Now $1 < f(1) = 2015$, and inductively $f^i(1) < f^{i+1}(1)$ for every positive integer i (where $f^i(X)$‘ denotes the composition of i copies of $f(X)$. It follows that $q(X) - q(1)$ has infinitely many roots $f^i(1)$ and so is the zero polynomial. Thus $q(X)$ is $u = q(1)$, a constant polynomial. Therefore $g = u(X - c) + c$.

Conversely if $g = u(X - c) + c$ for some constant u, then $f(g(X))$ is $uk(X - c) + c$ and this is also $g(f(X))$. The polynomials g which composition-commute with f are precisely the polynomials of degree at most 1 such that $g(c) = c$.

Now suppose that g is $u(X-c)+c$ and $h = v(X-c)+c$ are any two such polynomials, then $g(h(X)) = uv(X - c) + c = h(g(X))$ as required.