Math 2710

Nov 11-15

Functions

Definition: A function $f : A \to B$ is a subset $f \subset A \times B$ with the property that for every $a \in A$ there is exactly one b in B so that $(a, b) \in f$. We write $f : A \to B$ to mean that f is a function with domain A and co-domain B.

Compare this with the definition of a function as a "rule." The associated "rule" says: to compute $f(a)$, find the (uniquely determined) pair (a, b) in f, and then set $f(a) = b$.

In some sense this definition replaces the notion of a function with its graph.

Domain, co-Domain, Range

A is called the **DOMAIN** of f and B is called the **CO-DOMAIN.**

The **range** of f is the subset of b that occur in a pair $(a, b) \in f$.

A function can be drawn as a graph or as a "mapping" between two sets (see figure 12.3 in Hammack).

Examples

Consider problem 1 from Hammack. $A = \{0, 1, 2, 3, 4\}$ and $B = \{2, 3, 5, 6\}$. Then $f = \{(0, 3), (1, 3), (2, 4), (3, 2), (4, 2)\}$ Verify that f is a function and then find its range.

Is the subset of pairs of integers (x, y) where $3x + y = 4$ a function from $\mathbf{Z}$ to $\mathbf{Z}$?

Terminology: injective and surjective

Definition: A function is *injective* if it has the property that $f(a) \neq f(b)$ implies $a \neq b$. (or $f(a) = f(b)$ implies $a = b$). A function is *surjective* if for every $b \in B$ there is an a with $(a, b) \in f$. A function is *bijective* if it is both injective and surjective.

- *Injective* is also called "one-to-one." *Surjective* is also called "onto."
- Surjectivity depends on the codomain (you can shrink the codomain to make the function surjective).

Some examples

- $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ given by $f(n, m) = 2n - 4m$.

This function is not injective because $f(n, m)$ is always even; so for example $f(n, m) = 1$ has no solution. It is not injective because $f(4, 2) = f(0, 0) = 0$ so there are two different elements $a = (4, 2)$ and $b = (0, 0)$ in the domain with $f(a) = f(b)$.

- $f : \mathbb{Q} - \{2\} \to \mathbb{Q} - \{5\}$ given by $f(x) = (5x + 1)/(x - 2)$ is bijective.

To check surjectivity, you have to show that, if $y \in \mathbb{Q} - \{5\}$, then the equation $(5x + 1)/(x - 2) = y$ has a solution $x \in \mathbb{Q} - \{2\}$. Set $x = (-2y - 1)/(-y + 5)$. Since $y \neq 5$, this makes sense for any y in the codomain. Also the function on the right is never equal to 2, so the x is in the domain of the function.

more examples

- Consider maps from $\{0, 1, 2\}$ to $\{0, 1, 2\}$. how many are there? How many are injective? How many surjective? How many bijective?

Such a function is determined by its values on each element in the domain. To count the functions, you can send each of 0, 1, and 2 to any of 0, 1, and 2; so you have three choices of three things, for a total of $27 = 3^3$ functions. If the function is injective, then 0, 1, and 2 need to go to different things, so you have three choices for where to send 0, then 2 choices for where to send 1, and then 2 goes to whatever is left. That's a total of $3 \times 2 \times 1 = 6$ injective functions. If the function is surjective, then something has to hit 0 – there are three choices; something has to hit 1 – there are two choices left – and then whatever you haven't used must hit 2. So again there are $3 \times 2 \times 1 = 6$ maps. Implicit in this is the fact that in this case the surjective, injective, and bijective functions are all the same.

connection to number theory

Theorem: The function $f : \mathbb{Z}_m \to \mathbb{Z}_m$ given by $f(x) = ax$ is bijective if and only if $\gcd(a, m) = 1$.

First suppose that $\gcd(a, m) = 1$. We show that $f(x) = ax$ is injective. Suppose that $f(x) = f(y)$. This means that $ax \equiv ay \pmod{m}$. Since $\gcd(a, m) = 1$ we can cancel the a and see that $x \equiv y \pmod{m}$. Therefore f is injective (congruence means equality in $\mathbb{Z}_m$). To show that f is surjective, we must show that we can solve the equation $f(x) = y$ for any $y \in \mathbb{Z}_m$. This is the equation

$$ax \equiv y \pmod{m}$$

and by the theorem on linear congruences this has a solution when $\gcd(a, m) = 1$ since 1 divides y for any y.

Therefore if $\gcd(a, m) = 1$ the map f is surjective and injective and thus bijective.

number theory continued

Now we show that if the function is bijective then $\gcd(a, m) = 1$. It's a little easier to assume instead that $\gcd(a, m) \neq 1$ and prove that the function is not bijective. For this we can give counterexamples. Suppose $d = \gcd(a, m)$ and let $k = m/d$. Then $k \not\equiv 0 \pmod{m}$ (since $d > 1$ so $k < m$.) But $ak = am/d = (a/d)m \equiv 0 \pmod{m}$. So $f(k) = f(0)$ but $k \neq 0$ in $\mathbb{Z}_m$ so f is not injective. In fact, f is not surjective either. Since $d > 1$, by the theorem on congruences we cannot find $x \in \mathbb{Z}_m$ such that $ax \equiv 1 \pmod{m}$, so 1 is not in the range of f.

number theory continued

Theorem: Let a and b be integers with $b \neq 0$ and let $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be the function $f(x, y) = ax + by$. Then the range of f is the set of $n \in \mathbb{Z}$ such that $d = \gcd(a, b)$ divides n.

This is a restatement of (a part of) the theorem on linear diophantine equations. The range of f is the set of integers A such that $f(x, y) = A$ has a solution; and the theorem on diophantine equations tells us that this equation has a solution exactly when $d|A$.

Composition of functions

Definition: Suppose that $f : A \to B$ is a function and $g : B \to C$ is a function. The *composition* $g \circ f$ is a function from $A \to C$ defined by $(g \circ f)(a) = g(f(a))$.

This makes sense because $f(a) \in B$ and $g : B \to C$.

Examples:

- $f : \mathbf{R} \to \mathbf{R}$ given by $f(x) = x^2$, and $g : \mathbf{R} \to \mathbf{R}$ with $g(x) = \sin(x)$. What are $f \circ g$ and $g \circ f$?
- $A = \{0, 1, 2, 3\}$, $B = \{1, 2, 3, 4\}$, $C = \{1, 3, 5, 6\}$. $f = \{(0, 1), (1, 2), (2, 3), (3, 3)\}$ in $A \times B$. $g = \{(1, 3), (2, 3), (3, 3), 4, 3)\}$ in $B \times C$. What is the composition?

Properties of composition

Theorem: Composition of functions is associative.

Theorem: If $f : A \to B$ and $g : B \to C$ are injective then $g \circ f$ is injective. Similarly if f and g are surjective then $g \circ f$ is surjective. And if both are bijective, so is the composition.

Let's verify that if f and g are injective then so is $g \circ f$. Suppose $g(f(x)) = g(f(y))$. Then by injectivity of g we have $f(x) = f(y)$. By injectivity of f we have $x = y$. Therefore $g \circ f$ is injective.

The converse is false. Let $A = \{a, b\}$, let $B = \{0, 1, 2\}$, and let $C = \{u, v\}$. Define $f : A \to B$ by $f(a) = 0$, $f(b) = 1$. Define $g : B \to C$ by $g(0) = u$, $g(1) = v$, $g(2) = v$. Now $g \circ f$ sends $a \to u$ and $b \to v$ so it is injective; but g is not injective.

There is a partial converse:

Proposition: If $g \circ f$ is injective, then f is injective. If $g \circ f$ is surjective, then g is surjective.

Linear algebra

Someone asked in class about linear maps $f : \mathbf{R}^M \to \mathbf{R}^N$. In linear algebra you learned about the *rank* and the *nullity* of a linear map (or a matrix). The *rank* is the dimension of the range of f. The nullity is the dimension of the null space of f. An important basic theorem about linear maps is that *rank* plus *nullity* is the dimension of the domain of f.

The null space of f is the space of vectors that map to zero under f. If f were injective, then the only value that can map to zero is zero, so f is injective if and only if its nullity is zero.

If f is surjective, then its range must be equal to its codomain, so f is surjective if and only if the rank of f is n.

If f is bijective, then its rank must be n and its nullity must be zero; but this requires that $m = n$. So a linear map is bijective if $m = n$ and its nullity is zero or its rank is n.