Discrete Mathematics

Kenneth A. Ribet

January 31, 2013

A non-constructive proof

Two classical facts are that π and $e \approx 2.71828\ldots$ are irrational. Further, it is known that neither satisfies a quadratic equation $x^2 + ax + b = 0$ where a and b are both rational.

Theorem

The numbers $e\pi$ and $e + \pi$ are not both rational.

The proof is by contradiction. Assume that they are both rational, and let $a = \pi e$, $b = -(e + \pi)$. Then both π and e satisfy the equation $x^2 + ax + b = 0$, which is impossible (i.e., a contradiction).

The dispiriting thing is that we have no way of proving that $e\pi$ is irrational or that $e + \pi$ is irrational. We know only that they're not both rational. Pretty sad state of affairs!

Some sets

$A =$ the set of all students in the class.

$B = 2^A =$ the set of all sets of students in the class. The set B is called the *power set* of A and is denoted $\mathcal{P}(A)$ in the book.

Some elements of B: the set of all students who are present in lecture today; the set of all students in discussion section 108; the empty set $\emptyset$; the set of all students who are enrolled through concurrent enrollment; the set of all students who were born in Hawaii and have birth certificates to prove it.

Some standard sets

The set $\mathbf{Z}$ of all integers.

The set $\mathbf{Q}$ of rational numbers.

The set $\mathbf{C}$ of complex numbers.

The set $\mathbf{R}$ of real numbers.

The set $\mathbf{N}$ of natural numbers.

Wow: 0 is a natural number!! This is usually not true in North America.

Equality of sets

These are equal:

$$\{ x \in \mathbf{R} \mid x \geq 0 \} = \{ x^2 \mid x \in \mathbf{R} \}.$$

The point is that the two sets have the same elements. The descrptions may be different, but the sets are the same.

Subsets: $A \subseteq B$ means that every element of A is an element of B; the sets might be equal but aren't likely to be (whatever that means).

$A \subset B$ means that every element of A is an element of B and that we know for some reason that the “inclusion is strict." This means that there is at least one $b \in B$ that isn't in A.

The cardinality of a set S is denoted $|S|$ in the book. There are other plausible notations like $\#(S)$.

If S is finite, then $|S|$ is just the number of elements in S. For example, if S is the set of students enrolled in Math 55 as of 8:40PM on Wednesday evening, then $|S| = 211$.

If S is infinite, then we have to ruminate about the meaning of the cardinality of S.

If S has n elements, then $\mathcal{P}(S)$ has 2^n elements. This is true, for example, if $S = \emptyset$, in which case $n = 0$.

Cartesian products

For example, $A \times B$: this set consists of all pairs (a, b) with $a \in A$, $b \in B$.

For example, we could consider all pairs (s, n) where s is a US Senator and n is a natural number.

This might not be a fruitful activity.

Unions and intersections

You probably know that is meant by $A \cap B$ and $A \cup B$. When computing these, it is very helpful to think of A and B as subsets of some huge "universal" set U.

We can write $A \setminus B$ or even $A - B$ for the set of all elements of A that are not in B.

Especially when that makes sense. We could take A to be the set of all current UC Berkeley students who have ever taken Math 55 and B to be the set of all residents of Alameda County who have been arrested at least once in La Jolla.

We write $\bar{A}$ for $U - A$; here again, U is the universal set.

There is a list of “identities” like $\overline{(\overline{A})} = A$ on page 130 of the book.

These are mostly boring, but there are interesting identities like

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Functions

To give a function $f : A \to B$ is to specify an element $f(a)$ of B for each $a \in A$. What counts is the choices $f(a)$, not the "rule" that leads to $f(a)$.

For example, the function $\mathbf{R} \to \mathbf{R}$ that adds 1 to each $a \in \mathbf{R}$ and then subtracts 1 from the sum is the *same function* as the function that takes a to a ($=$ the identity function).

Never forget this!!!

Piazza question on the grading of quizzes

"Are these quizzes (1) graded on accuracy, (2) graded on effort, (3) not graded, or something else? Thanks!"

The GSIs and I have come to the following conclusions:

- There will be a quiz roughly every other week. The quiz questions will be made up by the individual GSIs.
- The quizzes will be graded carefully. Your grade will depend on the answer that you give and the English sentences that justify your answer. A typical question might be "Show that. . . ."
- I will maintain lists of quiz questions and will make them available to you on a web page so that everyone can see them and use them as practice questions for exams.
- Your quiz grade will count 0% of your course grade. The only purpose of the quizzes is to give you incremental feedback.

We could consider the function that assigns to each Math 55 student her student ID number (SID). For example, the fictional student Robert Joseph Birgeneau might have SID = 21930815 U 1.

If this function is $f : A \to B$, what is A and what is B?

Clearly A is the set of Math 55 students. The set B could be the set of "strings" of a certain length that consist of digits (0–9), capital letters (like "U") and spaces.

For mathematicians, it is very important that two functions f and g are considered to be the same function only when they have the same A and the same B and agree point by point on the set where they're both defined:

$$f(a) = g(a) \text{ for all } a \in A.$$

Consider $f : \mathbf{Z} \to \mathbf{Z}$ defined by $f(i) = i$ for all $i \in \mathbf{Z}$; this is the identity function on **Z.**

Compare with $g : \mathbf{Z} \to \mathbf{R}$ defined by $g(i) = i$ for all $i \in \mathbf{Z}$. This could be described as the natural inclusion of **Z** in **R.**

These are not the same function! The first one is surjective ("onto") but the second one isn't.

There is a lot of terminology associated with $f : A \to B$. The set A is the *domain* of f. Our book calls B the *codomain* of f. The set

$$f(A) = \{\, f(a) \mid a \in A \,\}$$

is called the *image* of f and sometimes also the *range* of f.

For $a \in A$, $f(a)$ is the *image* of a under f.

You probably know about *injective* ("1-1") functions as well as surjective functions.

For example, consider the doubling function $f : \mathbf{Z} \to \mathbf{Z}$ such that $f(n) = 2n$ for all $n \in \mathbf{Z}$. The *image* of this function is the set of even numbers. The function is 1-1 but not onto.

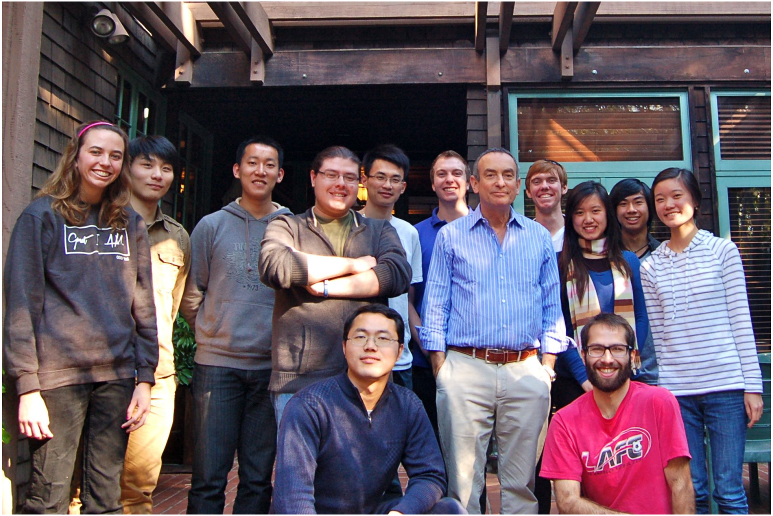
Or how about $g : \mathbf{Z} \to \mathbf{Z}$ defined by $g(n) = \lfloor n/2 \rfloor$; it takes n to the integer quotient of n by 2. This map is clearly onto but not 1-1.

For $n \in \mathbf{Z}$, we have $g(f(n)) = n$.

Faculty Club breakfast

A reminder that I will come to breakfast tomorrow at the Faculty Club at 7:30AM. Roughly two dozen of you are going to show up as well? Bring cash—$6 should do it.

We will be meeting in the Kerr Dining Room of the Club. No fancy dress is required. The cheap option is the “special breakfast” that includes two eggs, toast, coffee, orange juice, some fruit and more. It’s $3.99 plus tax plus tip; that’s how I came to $6.



Functions that are both 1-1 and onto are called *one-to-one correspondences*. A 1-1 correspondence is like a dictionary.

What's an interesting example? For example, we could try to have the function $d : \mathbf{R} \to B$ that assigns to each real number its decimal expansion. We can do the assignment uniquely if we avoid decimal expansions like $123.456999999\ldots$. (We'd use 123.457 in this case instead.) The set B would have to be carefully defined as a set of strings. The first element of each string would be a sign ($+$ or $-$), except that we'd have to make a special case for 0. Then there'd be a bunch of digits 0–9, possibly finitely many and possibly not. And a decimal point. This sounds potentially like a fruitful project.

We know in our hearts that real numbers are the "same" as decimals and the exercise would be to say in precise mathematical language what's going on.

If $f : A \to B$ is a 1-1 correspondence, its *inverse* f^{-1} is the function $B \to A$ that "undoes" f:

$$f^{-1}(b) = \text{ the unique } a \in A \text{ such that } f(a) = b.$$

For example, let $f : (-\pi/2, \pi/2) \to \mathbf{R}$ be the tangent function: $f(x) = \tan x$. Then f is a one-to-one correspondence whose inverse is the arctan function (often called $\tan^{-1}$).

For $f : A \to B$ and $g : B \to C$, we can define the composition of f and g, which is a map $A \to C$:

$$(g \circ f)(a) = g(f(a)).$$

We refer to $g \circ f$ as "f followed by g."

People in this country are used to reading from left to right and might find it strange that $g \circ f$ involves doing f first and then g second. That's life. It's always helpful to remember the construction $g(f(a))$. In mathematics (at least most of the time), functions are written to the left of their arguments.

Sometimes people write gf for the composition $g \circ f$.

This can lead to headaches. If f and g are numerical functions with the same codomain, we are sometimes led to write gf or fg for the pointwise product of f and g.

For example, suppose $f, g : \mathbf{R} \to \mathbf{R}$ as in Math 1A. It's very natural to write fg for the function $x \mapsto f(x)g(x)$. (Note the "$\mapsto$" character, which I'm using for the first time.) When people write $x \sin x$ they intend that the sin function and the identity function be multiplied, not composed.

The real lesson must be the notation can be flexible provided that everyone is on the same page.