MAU11602 Assignment 8, Due Wednesday 3 April 2024
Solutions

1. Suppose that S is a relation from A to B and R is a relation from B to C.

   (a) Show that if R and S are left unique then so is $R \circ S$.

   (b) Show that if R and S are right unique then so is $R \circ S$.

   (c) Show that if R and S are left total then so is $R \circ S$.

   (d) Show that if R and S are right total then so is $R \circ S$.

   (e) Show that if R and S are functions then then so is $R \circ S$.

   (f) Show that if R and S are injections then then so is $R \circ S$.

   (g) Show that if R and S are surjections then then so is $R \circ S$.

   (h) Show that if R and S are bijections then then so is $R \circ S$.

   Solution:

   (a) Suppose $(v, z) \in R \circ S$ and $(w, z) \in R \circ S$. In other words, there is an $x \in B$ such that $(v, x) \in S$ and $(x, z) \in R$ and there is a $y \in B$ such that $(w, y) \in S$ and $(y, z) \in R$. R is left unique so $x = y$. S is left unique so $v = w$. So if $(v, z) \in R \circ S$ and $(w, z) \in R \circ S$ then $v = w$. In other words, $R \circ S$ is left unique.

   (b) Suppose $(u, x) \in R \circ S$ and $(u, y) \in R \circ S$. In other words, there is an $v \in B$ such that $(u, v) \in S$ and $(v, x) \in R$ and there is a $w \in B$ such that $(v, w) \in S$ and $(w, y) \in R$. S is right unique so $v = w$. R is right unique so $x = y$. So if $(u, x) \in R \circ S$ and $(u, y) \in R \circ S$ then $x = y$. In other words, $R \circ S$ is right unique.

   (c) S is left total so for any $x \in A$ there is a $y \in B$ such that $(x, y) \in S$. R is left total so there is a $z \in C$ such that $(y, z) \in R$. By the definition of $R \circ S$ it follows that $(x, z) \in R \circ S$. Ro for every $x \in A$ there is a $z \in C$ such that $(x, z) \in R \circ S$. In other words, $R \circ S$ is left total.

   (d) R is right total so for any $z \in C$ there is a $y \in B$ such that $(y, z) \in R$. S is right total so there is an $x \in A$ such that $(x, y) \in S$. By the definition of $R \circ S$ it follows that $(x, z) \in R \circ S$. Ro for every $z \in C$ there is an $x \in A$ such that $(x, z) \in R \circ S$. In other words, $R \circ S$ is right total.

   (e) A function is just a relation which is left total and right unique.

   (f) An injection is just a relation which is left total and left and right unique.

   (g) A surjection is just a relation which is left and right total and right unique.

   (h) A bijection is just a relation which is left and right total and left and right unique.

2. Show that the set of real numbers is uncountable.
   Note: We haven't formally defined the real numbers in this module, and won't, so you can use an informal definition, like the fact that each (possible infinite) decimal expansion corresponds to a real number and vice versa, if we exclude the ones ending with all 9's. You don't need to give much detail on the parts of the proofs which are real analysis rather than set theory.
   Hint: You may find it convenient to use the fact that subsets of countable sets are countable.
   Solution: For each subset S of the natural numbers, i.e. member of PN, consider the sum

   $$f(S) = \sum_{j \in S} 10^{-j}.$$

   In other words, $f(S)$ has a 1 in the i'th digit of its decimal expansion to the right of the decimal point, assuming we start the count at 0, and has a 0 in all other positions, including to the left of the decimal point.

   If S and T are distinct sets, i.e. $S \neq T$, then $f(S) \neq f(T)$. This is kind of obvious but if you want to prove it then note that if $S \neq T$ then $S \setminus T$ or $T \setminus S$ is non-empty so there is a smallest i which is in one of them. If it's in $S \setminus T$ then $f(S) > f(T)$ and if it's in $T \setminus S$ then $f(S) < f(T)$. Let A be the range of f and R the set of real numbers. $A \subseteq R$ so if R were countable then A would be countable. In other words there would be an injective function g from A to N. $g \circ f$ would then be an injective function from PN to N. We already know there is no such function though, since PN is uncountable.

3. A number is called algebraic if is a root of a non-zero polynomial with rational coefficients. Using a counting argument, show that there are real numbers which are not algebraic.
   Note: You can use the result of the previous problem, even if you didn't manage to prove it.
   Solution: We know from the previous problem that the set of all reals is uncountable so it suffices to show that the set of algebraic reals is countable. There are a lot of ways to do this. The two most straightforward are the algebraic approach and the linguistic one.

   To each algebraic number we associate a list of natural numbers as follows. If a number is a root of a polynomial with rational coefficients then it is the root of a polynomial with integer coefficients, since we can always multiply an equation by the least common multiple of the denominators without changing the roots. Similarly we can divide by the greatest common divisor to make the coefficients relatively prime. Then we multiply the coefficients by -1, if necessary, to make the leading coefficent positive. That still doesn't identify a polynomial uniquely unless we also specify that it's of the lowest possible degree. If we do that then we have a polynomial relation

$$\sum_{j=0}^{n} c_j r^{n-j} = 0$$

satisfied by the algebraic number r, where the c's are integers and $c_0 > 0$. Since we're looking for a list of natural numbers rather than a list of integers we rewrite this as

$$\sum_{j=0}^{n} a_j r^{n-j} = \sum_{j=0}^{n} b_j r^{n-j}$$

where a_j is c_j if c_j is a natural number and 0 otherwise, while b_j is $-c_j$ if c_j is a negative integer and 0 otherwise. The list $(a_0, \ldots, a_n, b_0, \ldots b_n)$ isn't quite enough information to identify r uniquely though since there might be multiple real roots. So we prepend the number l to mean that r is the l'th solution to the equation as we move from left to right along the real line, i.e. from $-\infty$ to $+\infty$. So our final list of natural numbers is $(l, a_0, \ldots, a_n, b_0, \ldots b_n)$. We now have an injective function from the real algebraic numbers to the set of lists of natural numbers. Any set of lists with elements chosen from a countable set is countable, i.e. there is an injective function from it to the natural numbers. Composing, we get an injective function from the real algebraic numbers to the natural numbers, showing that the set of real algebraic numbers is countable.

If that proof seems to involve too much knowledge of algebra, there is another proof which requires almost none. For any real algebraic number there is at least one Boolean expression in the language of elementary arithmetic which describes it. For example $\sqrt{3}$ is the unique real number r satisfying

$$\{(r > 0) \wedge [(r \cdot r) = 0''']\}.$$

Previously we interpreted this language in such a way that the variables were all natural numbers, but we don't have to, and if we allow them to be real then the expression above is obviously satisfied by $\sqrt{3}$ and by no other number. There's nothing special about $\sqrt{3}$. We could do the same thing for any real algebraic number, giving an equation which it satisfies and a set of inequalities specifying an interval in which there are no other solutions to the equation. There may be, and indeed will be, many such expressions for any real algebraic number so we choose the one with the smallest encoding. Associating to each real algebraic number that smallest encoding gives us an injective function from the real algebraic numbers to the natural numbers, proving that the set is countable.

The advantage of the second proof is that it is easily adapted to show that essentially any set of objects each of which is uniquely describable in some language is countable, which is certainly not true of the first proof.