Supplementary notes - Proving that sets are countable

**Definition 1** A set \( A \) is countably infinite if there is a function \( f : A \to \mathbb{N} \) that is 1-1 and onto.

A good way to understand this definition is to realize that \( f \) gives rise to a listing of the elements of \( A \) in an infinite sequence \( a_0, a_1, \ldots \) (here \( a_i \) is the unique element \( a \) of \( A \) such that \( f(a) = i \)).

The key results for showing sets countable (other than explicitly constructing the function \( f \)) are:

1. An infinite subset of \( \mathbb{N} \) is countably infinite.
2. The union (finite or countable) of countably infinite sets is countably infinite.
3. The set of finite sequences of elements of a countable set is countably infinite.

Most of the proofs that sets \( A \) are countably infinite can be cast as corollaries or applications of these three key results. The first result above is usually used in tandem with the idea of “coding” or numbering a set. A coding of a set \( A \) is a method for associating to each element \( a \) of \( A \) a natural number that is based on the properties of \( a \) itself.

An example of a coding is the following proof of the countability of the rational numbers \( \mathbb{Q} \). Every rational number can be written as \(-1^n(a/b)\) where \( n \) is 0 or 1, \( a \) is a natural number, and \( b \) is a positive natural number. Furthermore, \( a \) and \( b \) have no common factor. Given such a rational number assign to it the “code” \( 2^n3^a5^b \). The key fact here is that two different rational numbers have different codes. Thus this coding is a 1-1 function mapping the rational numbers onto an infinite subset of \( \mathbb{N} \). By the first principle above, \( \mathbb{Q} \) is therefore countable.

**Problems**

1. As a warmup exercise, show that there are countably many integers. (The integers are the elements of the set \( \mathbb{Z} = \{ \ldots, -2, -1, 0, 1, 2, \ldots \} \).)
2. Let \( \text{FIN} \) denote the set of finite subsets of \( \mathbb{N} \). (So \( \{2, 4, 6\} \in \text{FIN} \) but the set of even numbers is not.) Show that \( \text{FIN} \) is countably infinite by constructing a coding.
3. Let \( \text{COF} \) denote the set of cofinite subsets of \( \mathbb{N} \). (A set is cofinite if it is the complement of a finite set. Thus \( \{n \mid n > 23\} \) is cofinite but the set of even numbers is not.) Show that \( \text{COF} \) is countably infinite.
4. A polynomial with integer coefficients is a function of form \( p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \) where \( a_0, a_1, \ldots, a_n \) are integers. Show that there are countably many polynomials with integer coefficients.
5. An algebraic number is any real number that is a root of a polynomial with integer coefficients.
   (a) Show that every rational number is an algebraic number.
   (b) Show that \( \sqrt{2} \) is an algebraic number.
   (c) Show that there are only countably many algebraic numbers.