0.4 Cardinality

:

In Section 10, the book introduce the formal axioms of the natural numbers. we need right now the Well Ordering Property.

The Well Ordering Property: Every nonempty subset $S \subseteq \mathbb{N}$ has a least element. In other words there exists $m \in S$ so that for all $k \in S$ $m \leq k$.

This property is simply assumed.

Example: If S is the even whole numbers then 2 is the least element.

Example: Consider S is the set of all prime numbers larger than 10^{10^6}. Such numbers have at least 1000,000 digits and are useful in coding. It is known by an argument that we may have time in later in this class that there are infinitely many primes. Therefore S has infinitely many members. The Well Ordering Principle assures that there is a smallest member of S. It does not say how to access it.

Historical Note: Leopold Kronecker (December 7, 1823 December 29, 1891) was a German mathematician and logician who argued that arithmetic and analysis must be founded on "whole numbers", saying, "God made the integers; all else is the work of man" (Bell 1986, p. 477).

Georg Ferdinand Ludwig Philipp Cantor (1845 1918) was a German mathematician, best known as the inventor of set theory, which has become a fundamental theory in mathematics. He was a professor at Halle, Province of Saxony 1867 on. Kronecker said of Cantor "scientific charlatan", a "renegade" and a "corrupter of youth." Cantor believed his theory of transfinite numbers had been communicated to him by God. Awarded the Sylvester medal (the highest honour) by the Royal Society in 1904 and defended by David Hilbert: "No one can expel us from the paradise that Cantor has created."

Definition: Two sets A and B are said to be *equinumerous* (or of equal cardinality) if there exists a bijection $f : A \to B$. We write $A \sim B$.

It is important here that $\mathrm{dom}(f) = A$ and $\mathrm{rng}(f) = B$ and that f is injective (1–1). Observe that if $\mathcal{F}$ is any set of sets then $\sim$ defines a relation S on $\mathcal{F}$: $(A, B) \in S$ if and only if $A \sim B$. The relationship "equinumerous" is an example of an equivalence relation.

Check that "$\sim$" is an equivalence relation on any family $\mathcal{F}$ of sets.

Lemma 0.1. *The relation "$\sim$" of "being equinumerous" is an equivalence relation on any family $\mathcal{F}$ of sets.*

Proof. We first check the relation is reflexive. Suppose A is a set. Is $A \sim A$? [Is there a bijection of A onto itself?] Yes the mapping $\iota_A : A \to A$ (the idenitity on A) defined by $\iota_A(a) = a$ for all $a \in A$ is a bijection.

Next check symmetry: Suppose A and B are two sets and $A \sim B$ so that there is a bijection $f : A \to B$. Is it true that $B \sim A$. Yes, choose $f^{-1} : B \to A$. Because f is a bijection, f^{-1} is also a bijection.

Finally we check transitivity: Suppose that $A \sim B$ and $B \sim C$ so that there are bijections $f : A \to B$ and $g : B \to C$. We want to show that $A \sim C$. However $g \circ f : A \to C$ is indeed a bijection by the previous result and so $A \sim C$. □

Remark Recall that equivalence classes are either disjoint or the same. One equivalence class would consist of all sets in $\mathcal{F}$ with 17 elements. Indeed for every finite number there is an equivalence class, namely all sets with that many elements. However cardinality also makes sense for infinite sets.

Definition: A set S is said to be *finite* if, either $S = \emptyset$ (in which case we say S has no elements) or if there exists $n \in \mathbb{N}$ and a bijection of S onto $\{1, 2, 3, \ldots n\}$ (in which case we say S has n elements.) If a set is not finite then it is *infinite*. The cardinal number of a finite set is the number of elements but the cardinal number of an infinite set is *transfinite*.

The book writes $I_n = \{1, 2, 3, \ldots, n\}$ for the archetypal set of cardinality n.

Lemma 0.2. *If $m > n$, $m, n \in \mathbb{N}$ then there is no injective mapping of I_m into I_n.*

Proof. For each $m \in \mathbb{N}$ let $P(m)$ be the statement: If there exists an injection $f : I_m \to I_n$ for some $n \in \mathbb{N}$ then $n \geq m$. We prove $P(m)$ for all $m \in \mathbb{N}$ by induction. $P(1)$ is the statement: If there is an injection $f : I_1 \to I_n$ for some $n \in \mathbb{N}$ then $n \geq 1$. Here there is nothing to check. $P(1)$ is true because $n \geq 1$ by virtue of the fact $n \in \mathbb{N}$.

Assume $P(k)$ for some $k \geq 1$, that is if there exists an injection $f : I_k \to I_n$ for some $n \in \mathbb{N}$ then $n \geq k$. To check $P(k+1)$, we suppose there is an injection $f : I_{k+1} \to I_n$ for some $n \in \mathbb{N}$. We would like to show that $n \geq k + 1$. Let us denote $f(k+1)$ by $n_0 \in I_n$: $n_0 = f(k+1)$. Define $g : I_k \to I_{n-1}$ by $g(j) = f(j)$ if $f(j) < n_0$ and $g(j) = f(j) - 1$ if $f(j) > n_0$. This assures that $g(j) \leq n - 1$, for all j, $1 \leq j \leq k$ because either $g(j) = f(j) < n_0 \leq n$ or $g(j) = f(j) - 1 \leq n - 1$ so indeed $g : I_k \to I_{n-1}$. Moreover g is 1–1. For suppose $g(j) = g(i)$ then there are two cases: one is $g(j) < n_0$ in which case $g(j) = f(j)$ and $g(i) = f(i)$ so that $f(i) = f(j)$ so that $i = j$ because f is 1–1; the second case is that $g(j) \geq n_0$, in which case $g(j) = f(j) - 1$ and $g(i) = f(i) - 1$ so that $f(i) = f(j)$ and again we conclude $i = j$ because f is 1–1. It now follows, by the induction hypothesis that $n - 1 \geq k$ or $n \geq k + 1$. This establishes $P(n)$ for all $n \in \mathbb{N}$ by induction. □

This assures us that finite cardinality behaves as one would expect. If one set A has cardinality n then it cannot also have cardinality $m \neq n$ where $m, n \in \mathbb{N}$. For supose that it did. Renaming m and n if necessary, we may suppose $m > n$. Then we would have two bijections $f : A \to I_n$ and $g : A \to I_m$. Then $f \circ g^{-1} : I_m \to I_n$ is a bijection and so 1–1 and this contradicts the Lemma. Therefore $m = n$.

It also says that $\mathbb{N}$ cannot be finite: if there were a 1–1 mapping of $\mathbb{N}$ to I_n for some n then the restriction of that mapping to I_m, $m > n$ would also be 1–1 and that is impossible by the Lemma.

Example: For example the mapping of $f : \mathbb{N} \to \{2, 4, 6, 8, \ldots\}$ defined by $f(n) = 2n$, for all $n \in \mathbb{N}$. Here $A = \mathbb{N}$; $B = \{2, 4, 6, 8, \ldots\}$. It is clear that f is 1-1 and onto and so the whole numbers and the even numbers have equal cardinality even though one is a proper subset of the other. This of course cannot happen with finite sets.

Definition: A set which is equinumerous with $\mathbb{N}$ is said to be *denumerable*. Any set which is either finite or denumerable, is said to be *countable*. Sets that are not countable are said to be *uncountable*.

What makes cardinality interesting is that there are uncountable sets and we will discover methods to distinguish which are countable and which uncountable.

Example: We have seen that the even numbers are denumerable and an easy argument shows that the odd numbers are countably infinite. What about the integers $\mathbb{Z} = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$? Try $f(n) = (-1)^n \lfloor x/2 \rfloor$ where $\lfloor m \rfloor$ denotes the greatest integer less or equal m. The verification that the mapping is 1–1 and onto is left to the reader.

Theorem 0.3. *A subset of a countable set is countable.*

Observe that the $\emptyset$ is considered to be finite and have 0 elements. This Theorem says that, for every subset T of a countable set S, there is a bijection of T onto $I_n = \{1, 2, 3, \ldots, n\}$ where n is the (finite) number of elements of S or there is a bijection of S onto $\mathbb{N}$.

Proof. Suppose that S is a countable set and $T \subseteq S$. Because S is countable there exists a bijection $f : S \to S'$ onto a $I_n = \{1, 2, 3, \ldots, n\}$ for some $n \in \mathbb{N}$ or onto $S' = \mathbb{N}$. We regard $I_n \subseteq \mathbb{N}$; indeed $\mathbb{N} = \cup_n I_n$ and so we can think of $S' \subseteq \mathbb{N}$. If T is void then T is countable: it has zero elements. Suppose therefore that $T \neq \emptyset$. Let $T' = \{f(t) : t \in T\}$ so that $T' \subseteq S' \subseteq \mathbb{N}$. It follows that T' has a least element t_1 by the Well Ordering Principle. If $T' = \{t_1\}$ then T and T' have one element and so are finite. (We map T to $I_1 = \{1\}$ in the obvious manner.) Otherwise $T' \backslash \{t_1\}$ is nonvoid in $\mathbb{N}$ and has a least element $t_2 > t_1$ by the W.O.P. Possibly $T' = \{t_1, t_2\}$ and this would say that T' and therefore T has two elements and we can define a bijection which takes $t_j \in T'$ to $j \in I_2$. Otherwise $T' \backslash \{t_1, t_2\}$ is nonvoid in $\mathbb{N}$ and so has a least element $t_3 > t_2$ again by the W.O.P. Proceeding in this way we either show that T' and therefore T have finitely many elements or there is a strictly increasing sequence $t_1 < t_2 < t_3 < \ldots < t_j < \ldots$ and the sequence goes on forever. In the latter case we define a mapping of $g : T' \to \mathbb{N}$ which takes t_j to $j$and that is clearly 1–1 and onto and so g is a bijection and so T' is countable. But $f : T \to T'$ is also a bijection and so this shows that if T is not finite it is equinumerous with $\mathbb{N}$ which is denumerable and so countable. In any case T is countable. □

Corollary 0.4. *If S is a set and there exists an injection of S into $\mathbb{N}$ then S is countable.*

Proof. The set S is equinumerous with $rng(f)$ where $f : S \to \mathbb{N}$ is the injection. By the previous Theorem, $rng(f)$ is countable. □

Theorem 0.5. *If A and B are countable then $A \times B$ is countable.*

Recall that $A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$.

Proof. We know that there is a bijection $f : A \to \mathbb{N}$ and another $g : B \to \mathbb{N}$. Consider the mapping

$$h(a, b) = 2^{f(a)}3^{g(b)}$$

so that $h : A \times B \to \mathbb{N}$. We check that h is $1-1$. To do so we note that if $2^j 3^k = 2^\ell 3^m$. Then $2^{j-\ell} = 3^{m-k}$ where we suppose that $j \geq \ell$ (or otherwise interchange j and ℓ. If $j \neq \ell$ then $2^{j-\ell}$ is even but 3^{m-k} cannot possibly be an even integer (product of odd numbers is odd). Therefore $j = \ell$ and so $m = k$. So h is $1 - 1$ because $h(a, b) = h(a', b')$ implies $f(a) = f(a')$ and $g(b) = g(b')$ and f and g are themselves $1 - 1$ so that $a = a'$, $b = b'$. Therefore $A \times B$ has the same cardinality as some subset of $\mathbb{N}$ and it is therefore countable. □

Remark The essence of the proof is to find a bijection of $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Can you do so directly? The mapping h above does not map onto $\mathbb{N}$.

Theorem 0.6. *The rational numbers form a countably infinite set.*

Proof. Every rational number can be written uniquely $\frac{\pm p}{q}$ where p and q are whole numbers and we assume that fractions are written in the lowest terms, for example $1/2$ and not $2/4$. More precisely any common factors in p and q are cancelled. Integers are written with $q = 1$. This shows that there is an injection $f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{N}$ defined by $f(p/q) = (p, q)$ of the rationals to a subset of $\mathbb{Z} \times \mathbb{N}$: $p/q \mapsto (p, q)$ and this correspondance is $1 - 1$ but not onto $\mathbb{Z} \times \mathbb{N}$. It follows that the rationals form a countably infinite set because we know that there is a bijection of the countable set $g : \mathbb{Z} \times \mathbb{N} \to \mathbb{N}$ by our ealrlier theorem (about the countability of $A \times B$) and so $g \circ f$ is a 1–1 mapping of $\mathbb{Q}$ into $\mathbb{N}$. $\mathbb{Q}$ is therefore countable. (An alternative argument is give on the top of page 83 of the Lay text.) □

Theorem 0.7. *(Theorem 8.10, Lay) Suppose that S is a nonempty set. Then the following are equivalent.*

1. *S is countable*
2. *There exists an injection $f : S \to \mathbb{N}$.*
3. *There exists a surjection $g : \mathbb{N} \to S$*

Proof. We saw the equivalence of part 1 and 2 above. Let us first show that $1 \Rightarrow 3$. Assume therefore that S is countable. It follows that S is either denumerable or finite. If S is denumerable then it is equinumerous with $\mathbb{N}$ and so there is a bijection $f : S \to \mathbb{N}$ and of course $g = f^{-1} : \mathbb{N} \to S$ is injective. If S is finite then there exists $n \in \mathbb{N}$ so that $S \sim I_n$ ($S \neq \emptyset$). Therefore there is a bijection $h : I_n \to S$. Define

$f : \mathbb{N} \to I_n$ by $f(k) = k$ if $1 \leq k \leq n$ and $f(k) = n$ if $k > n$. Certainly f is a surjection and therefore so is $h \circ f : \mathbb{N} \to S$: define $g = h \circ f$.

Conversely, suppose the $f : \mathbb{N} \to S$ is a surjection. Define $g : S \to \mathbb{N}$ as follows. For each $s \in S$ define $g(s) = \min\{k \in \mathbb{N} : f(k) = s\}$ observe that $\{k \in \mathbb{N} : f(k) = s\} \neq \emptyset$ simply because f is onto. Therefore the Well Ordering Principle tells us that $\{k \in \mathbb{N} : f(k) = s\}$ has a least element and we call that $g(s)$. Observe $f(g(s)) = s$. It follows that $g : S \to \mathbb{N}$ is injective because $g(s_1) = g(s_2)$ implies $s_1 = f(g(s_1)) = f(g(s_2)) = s_2$. It follws by the equivalence of parts 1 and 2 of this result that S must be countable. □

Theorem 0.8. *If $\mathcal{A}$ is a countable set and for every $\alpha \in \mathcal{A}$, S_α is a countable set. Then*

$$\cup_{\alpha\in\mathcal{A}} S_\alpha \text{ is countable}$$

Proof. We will show that there is a surjection $f : \mathbb{N} \times \mathbb{N} \to \cup_{\alpha\in\mathcal{A}} S_\alpha$. This will complete the proof because we already know that $\mathbb{N} \times \mathbb{N}$ is denumerable and so there is a bijection, $G : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ and so $f \circ G : \mathbb{N} \to \cup_{\alpha\in\mathcal{A}} S_\alpha$ would be surjective and so the $\cup_{\alpha\in\mathcal{A}} S_\alpha$ would be countable by the previous result. (Note the difficulty with counting $\cup_{\alpha\in\mathcal{A}} S_\alpha$ is that there is no way of knowing how much overlap there is between S_α's.)

We define f as follows. We know there is a surjection $h : \mathbb{N} \to \mathcal{A}$, by the previous result because $\mathcal{A}$ is a countable set. For each $\alpha \in \mathcal{A}$ there is a surjection $g_\alpha : \mathbb{N} \to S_\alpha$. Define $f : \mathbb{N} \times \mathbb{N} \to \cup_{\alpha\in\mathcal{A}} S_\alpha$ by

$$f(m, n) = g_{h(m)}(n)$$

We need to check that this is surjective. Suppose therefore that $s \in \cup_{\alpha\in\mathcal{A}} S_\alpha$. This means that there exists $\alpha \in \mathcal{A}$ so that $s \in S_\alpha$. Because h is surjective there is $m \in \mathbb{N}$ so $h(m) = \alpha$ and because $g_{h(m)} = g_\alpha$ is surjective (onto S_α) there is $n \in \mathbb{N}$ so that $g_{h(m)}(n) = s$ and this just says $f(m, n) = s$ and this checks that f is onto and completes the proof. □

Theorem 0.9. *The real numbers are an uncountably infinite set.*

Proof. We shall prove that $(0, 1)$ is not countable and that will establish the result. We shall identify a real number x has a decimal expansion. The decimal expansion is unique except if the expansion terminates in all zeroes or all nines. For example $0.4999999999999 \ldots = 0.5$. We can assume that all decimal expansions that terminate in all nines are converted to all zeroes.

Suppose that there is an enumeration $f(n)$, $n \in \mathbb{N}$ of the reals: so that $f : \mathbb{N} \to$

$(0,1)$ is one to one and onto. Let us list the values of $f(n)$ in decimal form

$$\begin{aligned} f(1) &= 0.d_{1,1}d_{1,2}d_{1,3}d_{1,4}\dots \\ f(2) &= 0.d_{2,1}d_{2,2}d_{2,3}d_{2,4}\dots \\ f(3) &= 0.d_{3,1}d_{3,2}d_{3,3}d_{3,4}\dots \\ f(4) &= 0.d_{4,1}d_{4,2}d_{4,3}d_{4,4}\dots \\ \vdots &\ \vdots\ \vdots \end{aligned}$$

where each $d_{i,j}$ is a digit $0 \leq d_{i,j} \leq 9$. Let us define a real number $r = 0.d_1d_2d_3d_4\dots$ as follows. We shall change the digits $d_{n,n}$ that appear on the main diagonal to make up the new number r. More precisely, if $d_{1,1} \leq 4$ then we define $d_1 = d_{1,1} + 4$ and otherwise $d_1 = d_{1,1} - 4$. It follows that $|r - f(1)| \geq 0.3$ no matter what the remaining digits of r or $f(1)$ are. This is because the largest change one can make in a number by changing the digits after the tenths digit is 0.1 =0.09999999999. WE also see that $1 \leq d_1 \leq 8$ Define $d_2 = d_{2,2} + 4$ if $d_{2,2} \leq 4$ and $d_2 = d_{2,2} - 4$ otherwise. Observe that $|0.d_{2,1}d_{2,2} - 0.d_1d_2| \geq 0.04$ so that $|f(2) - r| \geq 0.03$. Continue in this way. d_n is defined to be $d_{n,n} + 4$ if $d_{n,n} \leq 4$ and $d_n = d_{n,n} - 4$ otherwise. This choice forces $r \neq f(n)$. Inductively we define all the digits d_n of r so that $|d_n - d_{n,n}| = 4$ we will have $r \neq f(n)$. In the end we have constructed a number r, $0 < r < 1$ which is not equal to $f(n)$ for any n and this contradicts the assumption that f enumerates (is onto) (0,1). (0,1) is uncountable. □

This is referred to as the "diagonal argument" and although the result is due to Cantor, this proof is not. Of course by one of the problems in the homework, all real intervals (a,b), where $a < b$ are uncountable.

Corollary 0.10. *The set of all irrational numbers in an open interval (a,b), $a < b$ is uncountable.*

Proof. We know that $(a,b) = (\mathbb{Q} \cap (a,b)) \cup (\mathbb{Q}^c \cap (a,b))$ and we know $(\mathbb{Q} \cap (a,b))$ is countable as a subset of a countable set. If $(\mathbb{Q}^c \cap (a,b))$ were also countable then the union (a,b) would also be countable by our earlier result but that contradicts the Theorem. □

Recall that the power set $\mathcal{P}(s)$ of a set S consists of all subsets of $\mathcal{S}$

Theorem 0.11. *For any set S, the power set $\mathcal{P}(S)$ is not equinumerous with S.*

Proof. The proof is by contradiction. Suppose to the contrary there is a bijection $f : S \to \mathcal{P}(S)$. Define

$$T = \{s \in S : s \notin f(s)\}$$

Since f is a bijection there is $t \in S$ so that $f(t) = T$. We ask the question is $t \in T$? If $t \in T$ then by the definition of T, $t \notin f(t)$ but $f(t) = T$ and so this is absurd. Therefore $t \notin T$ but then $t \notin f(t)$ and this assures that $t \in T$ and so we have a contradiction. There cannot be a bijection of s onot $\mathcal{P}(S)$. □

Remark: We have an ordering $1 < 2 < 3 < 4 < \ldots < \aleph_0 < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N})| < \ldots$. In other words we have constructed and infinite number of distinct transfinite cardinals.

Definition: The cardinality of $\mathbb{R}$ is called the continuum and is written c.

It can be shown (Exercise 8.24) $c = |\mathcal{P}(\mathbb{N})|$

Continuum Hypothesis: There is no cardinal λ so that $\aleph_0 < \lambda < c$.

This conjecture is due to Cantor and it is Problem 1 of the 23 problems proposed by David Hilbert (1862-1943) at the International Congress of Mathematicians in Paris in 1900. It has been shown that the continuum hypothesis is consistent with the usual axioms of set theory (Kurt Gödel, 1938) and its negation is too (Paul Cohen 1963).