Sets and their properties

Written by Paul Schrimpf and modified by Hiro Kasahara
August 31, 2020
University of British Columbia
Economics 526

Much (perhaps all) of mathematics is about studying sets of objects with particular properties.

Section 1 introduces sets and some related concepts. Section 1.4 briefly discusses cardinality and introduces countable and uncountable sets. Section 2 is about relations, especially orders, which are used to state Arrow's impossibility theorem. The appendix section A is about familiar sets of numbers, including the integers, rationals, and real numbers. The properties of these sets of numbers that make them distinct are discussed.

References. Section 1 on sets is partly based on chapter 1 of Carter (2001). Any similar high-level mathematical economics textbook covers similar material. Examples include De la Fuente (2000), Ok (2007), and Corbae, Stinchcombe, and Zeman (2009). Textbooks on real analysis, such as Rudin (1976) and Tao (2006), also typically start with a section about sets.

Section 1.4 about cardinality is largely based on chapter 2 Rudin (1976). Chapter B of Ok (2007) covers similar material. Weeks 2 and 3 of the notes of Tao (2003) (on which Tao (2006) is based) also cover cardinality.

Section 2 about relations is based on chapter 1.2 of Carter (2001). Arrow's impossibility theorem first appeared in Arrow (1950). Feldman (1974) is a more approachable, simplified proof of the theorem.

The appendix section A is based on Rudin (1976), but any textbook on real analysis will cover similar material. Tao (2006) (or the note version Tao (2003)) is especially detailed and careful in its construction of the real numbers.

1. Sets

A **set** is any well-specified collection of elements.[1] Sets are conventionally denoted by capital letters, and elements of a set are usually denoted by lower case letters. The notation, $a \in A$, means that a is a member of the set A. A set can be defined by listing its elements inside braces. For example,

$$A = \{4, 5, 6\}$$

[1] "Well-specified" is somewhat ambiguous, and this ambiguity can lead to trouble such as Russell's paradox or Cantor's paradox. We'll ignore these paradoxes, but rest assured that they can be avoided by more carefully defining "well-specified."

means that A is a set of three elements with members 4, 5, and 6. The members of a set need not be explicitly listed. Instead, they can be defined by some logical relation. For example, the same set A could be written

$$A = \{n \in \mathbb{N} : 3 < n < 7\} \tag{1}$$

where $\mathbb{N} = \{1, 2, 3, ...\}$ is the natural numbers. The expression in (1) could be read as, "the set of natural numbers, n, such that 3 is less than n is less than 7." Sometimes $|$ will be used to mean "such that" instead of $:$. The elements of sets need not be simple things like numbers. For example, if $A_k = \{n \in \mathbb{N} : n > k\}$ is the set of natural numbers greater than k, then you could have a set of sets, $B = \{A_1, A_{10}, A_6\}$. Sets are unordered, so the previous definition of B is the same as $B = \{A_1, A_6, A_{10}\}$. Also, sets do not contain duplicates, so for example, $\{1, 1, 2\} \equiv \{1, 2\}$. Sets can be empty. The empty set, also called the null set, is denoted by $\emptyset$ or, less commonly, $\{\}$.

1.1. **Economic examples.** Sets appear all over economics.[2]

Example 1.1. [Sample space] In a random experiment, the set of all possible outcomes is called the **sample space**. E.g. for the roll of a dice, the sample space if $\{1, 2, 3, 4, 5, 6\}$. An **event** is any subset of the sample space.

Example 1.2. [Games] A game is a model of strategic decision making. A game consists of a finite set of n players, say $N = \{1, 2, ..., n\}$. Each player $i \in N$ chooses an action a_i from a set of actions A_i. The outcome of the game depends on the actions chosen by all players.

Example 1.3. [Consumption set] The **consumption set** is the set of all feasible consumption bundles. Suppose there are n commodities. A consumer chooses a consumption bundle $\mathbf{x} = (x_1, x_2, ..., x_n)$. Consumption cannot be negative, so the consumption set is a subset of $\mathbb{R}^n_+ = \{(x_1, ..., x_n) : x_1 \geq 0, x_2 \geq 0, ...x_n \geq 0\}$.

1.2. **Set operations.** Given two sets A and B, a new set can be formed with the following operations:

(1) **Union:** $A \cup B = \{x : x \in A \text{ or } x \in B\}$.
(2) **Intersect:** $A \cap B = \{x : x \in A \text{ and } x \in B\}$.
(3) **Minus:** $A \setminus B = \{x : x \in A \text{ and } \notin B\}$
(4) **Product:** $A \times B = \{(x, y) : x \in A, y \in B\}$
(5) **Power set:** $\mathcal{P}(A) =$ set of all subsets of A

Often, we will discuss sets that are all subsets of some universal set, U. In this case, the **complement** of A in U is $A^c = U \setminus A$. If we have an indexed collection of sets, $\{A_k\}_{k \in \mathcal{K}}$, we may take the union or intersection of all these sets and denote it as $\cup_{k \in \mathcal{K}} A_k$ or $\cap_{k \in \mathcal{K}} A_k$.

[2]These examples come from chapter 1 of Carter.

1.3. **Set relations.** If every element of A is also in B, then we say that B contains A and write $B \supseteq A$, or A is a subset of B and write $A \subseteq B$. If, additionally, there exists $b \in B$ such that $b \notin A$, then we say that A is a proper subset of B, which is denoted by $A \subset B$ or $B \supset A$.

Example 1.4 (1.2 Games continued)**.** In a game subsets of players are called **coalitions**. The set of all coalitions is the power set of the set of players, $\mathcal{P}(N)$.

The **action space** of a game is the set of all possible outcomes or combinations of actions, $A = A_1 \times A_2 \times ... \times A_n$. An element of A, $a = (a_1, a_2, ..., a_n)$ is called an **action profile**.

1.4. **Cardinality .** [3] Sometimes, we want to compare the size of two sets. This is easy when sets are finite; we simply count how many elements each has. It is not so easy to compare the size of infinite sets. Consider, for example, the natural numbers, $\mathbb{N}$, the integers $\mathbb{Z}$, rationals, $\mathbb{Q}$, and real numbers, $\mathbb{R}$. Let $|A|$ denote the "size" of A (we will define it precisely later). We know that

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R},$$

so it seems sensible to say that

$$|\mathbb{N}| < |\mathbb{Z}| < |\mathbb{Q}| < |\mathbb{R}|.$$

On the other hand, the even integers are a subset of $\mathbb{Z}$, but since we can write the set of even integers as $\{2x : x \in \mathbb{Z}\}$, it doesn't seem like there are any more integers than even integers. It was questions like these that led Georg Cantor to pioneer set theory in the 1870's.

A function (aka mapping), $f : A \to B$ is called **one-to-one** (aka injective) if for every $b \in B$ the set $\{a : f(a) = b\}$ is either a singleton or emptyo. f is called **onto** (aka surjective) if $\forall b \in B\ \exists a \in A : f(a) = b$. If there exists a one-to-one mapping of A onto B (aka bijection or one-to-one correspondence), then we say that A and B have the same **cardinal number** (or cardinality) and write $|A| = |B|$. Let $J_n = \{1, ..., n\}$. A is **finite** if $|A| = |J_n|$. A is **countable** if $|A| = |\mathbb{N}|$. A is **uncountable** if A is neither finite nor countable. You should verify that the relation $|A| = |B|$ is reflexive ($|A| = |A|$), symmetric ($|A| = |B|$ implies $|B| = |A|$), and transitive (if $|A| = |B|$ and $|B| = |C|$ then $|A| = |C|$).

Lemma 1.1. *$\mathbb{Z}$ is countable.*

Proof. We can construct a bijection between $\mathbb{Z}$ and $\mathbb{N}$ as follows:

$$\begin{array}{lccccccc} \mathbb{Z}: & 0, & -1, & 1, & 2, & -2, & 3, & -3, ... \\ \mathbb{N}: & 1, & 2, & 3, & 4, & 5, & 6, & 7, ... \end{array}$$

Or as a formula, $f : \mathbb{N} \to \mathbb{Z}$ with

$$f(n) = \begin{cases} (n-1)/2 \text{ if } n \text{ odd} \\ -n/2 \text{ if } n \text{ even.} \end{cases}$$

□

[3] This section based on Chapter 2 Rudin (1976).

Theorem 1.1. *Every infinite subset of a countable set A is countable.*

Proof. A is countable, so there exists a bijection from A to $\mathbb{N}$. We can use this mapping to arrange the elements of A in a sequence, $\{a_n\}_{n=1}^{\infty}$[4]. Let B be an infinite subset of A. Let n_1 be the smallest number such that $a_{n_1} \in B$. Given n_{k-1}, let n_k be the smallest number greater than n_{k-1} such that $a_{n_k} \in B$. Such an n_k always exists since B is infinite. Also, $B = \{a_{n_k}\}_{k=1}^{\infty}$ since otherwise there would be a $b \in B$, but $b \notin A$. Thus, $f(k) = a_{n_k}$ is a one-to-one correspondence between B and $\mathbb{N}$. □

Theorem 1.2. *The rational numbers are countable.*

Proof. Consider the following arrangement of positive rational numbers:

$$\begin{matrix} 1/1 & 2/1 & 3/1 & 4/1 & \cdots \\ 1/2 & 2/2 & 3/2 & 4/2 & \cdots \\ 1/3 & 2/3 & 3/3 & 4/3 & \cdots \\ \vdots & & & \ddots & \end{matrix}$$

Starting in the top left and going back and forth diagonally, we get the following sequence:

$$1/1, 1/2, 2/1, 1/3, 2/2, 3/1, \ldots$$

Adding zero and the negative rationals, we can write e.g.

$$\begin{aligned} &0, 1/1, -1/1, 1/2, -1/2, 2/1, -2/1, 1/3, -1/3, 2/2, -2/2, 3/1, \ldots \\ =&q_1, q_2, q_3, q_4, \ldots \end{aligned}$$

Continuing on in this way, we could list all rational numbers. Some of these fractions represent the same number and can be removed. Thus, we obtain a correspondence between the rationals and an infinite subset of $\mathbb{N}$. However, by theorem 1.1, this subset is countable, so the rationals are also countable. □

Theorem 1.3. *The real numbers are uncountable.*

Proof. (Cantor's diagonal argument) We have not rigorously defined the real numbers, so we will take for granted the following: every infinite decimal expansion, (e.g. 0.135436080...) represents a unique real number in $[0, 1)$, except for expansions that end in all zeros or nines, which are equivalent[5].

We will use proof by contradiction to prove the theorem. Proof by contradiction is a common technique that works by showing that if the theorem were false, then we could prove something that contradicts what we know is true.

[4]By this notation, we mean an infinite ordered list of elements of A, i.e. $a_1, a_2, a_3, \ldots$.

[5]E.g. 0.199... = 0.200...

Suppose the theorem is false. Then we can construct a surjective mapping from $\mathbb{N}$ to $(0,1)$. That is we can list all real numbers in $(0,1)$ as

$$\begin{array}{llllll} r_1 & = 0. & d_{11} & d_{12} & d_{13} & \dots \\ r_2 & = 0. & d_{21} & d_{22} & d_{23} & \dots \\ r_3 & = 0. & d_{31} & d_{32} & d_{33} & \dots \\ \vdots & & \vdots & & & \end{array}$$

where each $d_{ij} \in \{0, 1, \dots, 9\}$, and no expansion ends in all nines. We will now show that there is a real number in $(0,1)$ that is not in the list. Let $x^* = 0.d_1^* d_2^* d_3^* \dots$ where d_n^* is chosen such that $d_n^* \neq d_{nn}$ and x^* is sure not to end in all nines. There are many possibilities, but to be concrete, let's set

$$d_n^* = \begin{cases} d_{nn} + 1 \text{ if } d_{nn} < 8 \\ 0 \text{ if } d_{nn} \geq 8 \end{cases}.$$

x^* is in $(0,1)$, but $x^* \neq r_n$ for any n because $d_n^* \neq d_{nn}$. Thus, we have a contradiction, and there cannot be a onto mapping from $\mathbb{N}$ to $(0,1)$. If there is no surjective mapping from $\mathbb{N}$ to $(0,1)$, there can be no surjective mapping from $\mathbb{N}$ to $\mathbb{R}$ since $(0,1) \subset \mathbb{R}$. □

Countable sets are said to have cardinality $\aleph_0$ ("aleph null"). Note that an implication of theorem 1.1 is that $\aleph_0$ is the smallest infinite cardinal number. The real numbers have cardinality of the continuum, sometimes written $2^{\aleph_0}$ or $\mathbf{c}$. You might be wondering whether there are larger cardinal numbers. The answer is yes. The set of all subsets of a set, A, called the **power set** of A, always has larger cardinality $2^{|A|}$ (the proof of this is similar to the proof that the real numbers are uncountable).

A final question to ask yourself is whether there are sets with cardinality between $\aleph_0$ and $2^{\aleph_0}$. The answer to that question is whatever you want it to be. The conjecture that there are no cardinal numbers between $\aleph_0$ and $2^{\aleph_0}$ is known as the continuum hypothesis. It was proposed by Cantor in the 1870s. In 1900, Hilbert made a famous list of 23 important unsolved problems in mathematics. The continuum hypothesis was the first. In 1940, Gödel showed that the continuum hypothesis cannot be disproved from the standard axioms that lie at the foundation of mathematics. In 1963, Cohen showed that the continuum hypothesis cannot be proved from the standard axioms. This is an example of Gödel's incompleteness theorem, a very interesting result that we won't be able to cover in this course. Loosely speaking, Gödel's incompleteness theorem says that for any non-trivial set of assumptions and system of logic, you can make statements consistent with the system of logic that cannot be proven or disproven from the assumptions.

Appendix A. Numbers

We have been assuming familiarity with the natural numbers, integers, rationals, and real numbers. This section explores some properties of these sets of numbers and heuristically describes how these sets of numbers are constructed. It may appear silly and slightly confusing to try to be "rigorous" about something like real numbers that we already feel like we understand. Much of mathematics is about finding and describing patterns that apply to abstract objects. Many of the abstract objects that we will study are similar to the real numbers in some ways, but different in others. Examples of things that are similar to the real numbers include complex numbers, vector spaces, matrices, and sets of functions. Some of these things we will be able to add and multiple just like real numbers, but not all of them. A natural sort of question is: this class of objects shares properties X, Y, and Z with the real numbers; what theorems that we know about the real numbers will also be true of this class of objects? Before answering this sort of question we have to be precise about what properties the real numbers have.

We will take for granted that we understand what the natural numbers are. Note, however, that it is possible to rigorously construct the natural numbers from a simple list of assumptions using logic or set theory. We will also take for given that we know how to add and multiply natural numbers. Addition has the following nice properties.

1 *Closure* if $a, b \in \mathbb{N}$, so is $a + b$
2 *Associative* $a + (b + c) = (a + b) + c$.

If we demand that addition also has

3 *Identity* $\exists 0$ s.t. $a + 0 = a$,
4 *Inverse* $\forall a$, $\exists b$ s.t. $a + b = 0$

then we must expand the natural numbers to include the integers, $\mathbb{Z}$. Multiplication also satisfies these four analogous properties:

1′ *Closure* if $a, b \in A$, so is ab
2′ *Associative* $a(bc) = (ab)c$.
3′ *Identity* $\exists 1$ s.t. $a1 = a$,
4′ *Inverse* $\forall a \neq 0$, $\exists b$ s.t. $ab = 1$

However, if we want multiplicative inverses to exist for all $z \in \mathbb{Z}$, then we must further expand our set of numbers to the rationals, $\mathbb{Q}$. Addition and multiplication are also

5 *Commutative* $a + b = b + a$
6 *Distributive* $a(b + c) = ab + ac$

To summarize: if we start with the natural numbers, and then demand that multiplication and addition have these six properties, we end up with the rational numbers.

More generally, we could study a set A combined with one or two operations that satisfy certain properties. The branch of mathematics that studies these sort of objects is abstract algebra. We will not be studying algebra in detail, but it may be useful to be familiar with some basic terms. A **group** is a set and operation, $(A, \oplus)$ such that A is closed under $\oplus$, $\oplus$ is associative, there exists an identity, and inverses exist under $\oplus$ (i.e. properties 1-4). If $\oplus$ is also commutative, we call $(A, \oplus)$ an abelian (or commutative) group. Examples of groups include $(\mathbb{Z}, +)$ and $(\mathbb{Q}, \cdot)$. A **ring** is a set with two operations, $(A, \oplus, \odot)$ such that $(A, \oplus)$ is a group, and $\odot$ has properties 1-3 and 6. $(\mathbb{Z}, +, \cdot)$ is a ring. One ring that will come up repeatedly in this course is the set of all n by n matrices with the usual matrix addition and multiplication. A **field** is a set with two operations such that 1-6 hold for both operations. $(\mathbb{Q}, +, \cdot)$ is a field. Another field that you may have encountered is the complex numbers with the usual addition and multiplication. If you're interested you may want to verify that the integers modulo any number is a ring, and the integers modulo any prime number if a field.

A.1. **Real numbers.** The rational numbers are pretty nice; they're a field with the six properties listed above. However, $\mathbb{Q}$ does not contain all the numbers that we think it should. For example,

Theorem A.1. $\sqrt{2} \notin \mathbb{Q}$

Proof. Suppose $\sqrt{2} \in \mathbb{Q}$. Then $\sqrt{2} = p/q$ where p and q are not both even. If we square both sides, we get

$$2 = p^2/q^2$$
$$2q^2 = p^2.$$

Hence, p^2 must be even. From the review, then p must also be even, say $p = 2m$. Then we have

$$2q^2 = 2(2m^2)$$
$$q^2 = 2m^2,$$

which means q must also be even, contrary to our starting assumption. □

Apparently, the rationals have some holes in them that we should fill in. To do so in a unique way, we need to define another property of the rational numbers. A **totally ordered set** is a set, A, and a relation, $<$, such that (i) (total) $\forall a, b \in A$ either $a < b$ or $a = b$ or $a > b$; and (ii) (transitive) if $a < b$ and $b < c$ then $a < c$. An **ordered field** is a field that is a totally ordered set and addition and multiplication preserve the ordering in that (i) if $b < c$ then $a + b < a + c$ (ii) if $a > 0$ and $b > 0$ then $ab > 0$.

We need one more definition. Simon and Blume state that one property of real numbers that will be used throughout the book is the least upper bound property. It turns out that this property is not only useful; it lies at the foundation of the real numbers. Let S be an ordered set and $A \subset S$. $s \in S$ is an **upper bound** of A if $s \geq a \forall a \in A$. s is a **least upper bound** (aka supremum) of A if s is an upper bound of A and if $r < s$, then r is not an upper bound of A. S has the **least-upper-bound property** (aka complete or Dedekind complete) if whenever $A \subset S$ has an upper bound, A has a least upper bound. Given that $\sqrt{2} \notin \mathbb{Q}$, it should not be surprising that the rational numbers are not complete.

Theorem A.2 (Real numbers)**.** *There exists an ordered field, $\mathbb{R}$, that has the least upper bound property. $\mathbb{R}$ contains $\mathbb{Q}$. Moreoever, $\mathbb{R}$ is "unique".*

The proof of this is surprisingly long, so we will not go over it in detail. Existence can be proven by construction. One method involves constructing real numbers as Dedekind cuts. A Dedekind cut is a nonempty subset of the rationals, $A \subset \mathbb{Q}$, such that (i) if $p \in A$, $q \in \mathbb{Q}$, and $q < p$, then $q \in A$ and (ii) if $p \in A$ then $p < r$ for some $r \in A$ (i.e. A has no greatest element. For example, the Dedekind cut associated with $\sqrt{2}$ would be $\{p \in \mathbb{Q} : p^2 < 2\}$). We would then define addition, multiplication, and ordering of these cuts in the natural way and verify that all the properties above are satisfied. See Rudin (1976) for details if you are interested.

The "uniqueness" is harder to prove. $\mathbb{R}$ is unique in the sense that any two ordered fields with the least-upper-bound property are isomorphic (there exists a bijection between them that preserves multiplication, addition, and ordering). The proof proceeds by supposing that $\mathbb{R}$ and $\mathbb{F}$ are two ordered fields with the least-upper-bound property and then shows that there is an isomorphism between them.

References

Arrow, Kenneth J. 1950. "A Difficulty in the Concept of Social Welfare." *Journal of Political Economy* 58 (4):pp. 328–346. URL http://www.jstor.org/stable/1828886.

Carter, Michael. 2001. *Foundations of mathematical economics*. MIT Press.

Corbae, Dean, Maxwell B Stinchcombe, and Juraj Zeman. 2009. *An introduction to mathematical analysis for economic theory and econometrics*. Princeton University Press.

De la Fuente, Angel. 2000. *Mathematical methods and models for economists*. Cambridge University Press.

Feldman, Allan M. 1974. "A VERY UNSUBTLE VERSION OF ARROW'S IMPOSSIBILITY THEOREM." *Economic Inquiry* 12 (4):534–546. URL http://dx.doi.org/10.1111/j.1465-7295.1974.tb00420.x.

Ok, Efe A. 2007. *Real analysis with economic applications*, vol. 10. Princeton University Press.

Rudin, Walter. 1976. *Principles of Mathematical Analysis (International Series in Pure & Applied Mathematics)*. McGraw-Hill Publishing Co.

Tao, Terence. 2003. "Math 131AH." URL http://www.math.ucla.edu/~tao/resource/general/131ah.1.03w/.

———. 2006. *Analysis*, vol. 1. Springer.