Cardinality rationals reals

Comparing $\mathbb{Q}$ and $\mathbb{R}$

Both $\mathbb{Q}$ and $\mathbb{R}$ have no greatest element.

Both $\mathbb{Q}$ and $\mathbb{R}$ have no least element.

The quantified statement

$$\forall x \forall y (x < y \to \exists z (x < z < y))$$

is true about both $\mathbb{Q}$ and $\mathbb{R}$.

Both $\mathbb{Q}$ and $\mathbb{R}$ are infinite. But, $\mathbb{Q}$ is countably infinite whereas $\mathbb{R}$ is uncountable.

The set of real numbers

$\mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$

Order axioms (Rosen Appendix 1):

Reflexivity	$\forall a \in \mathbb{R}(a \leq a)$
Antisymmetry	$\forall a \in \mathbb{R}\ \forall b \in \mathbb{R}\ (\ (a \leq b\ \wedge\ b \leq a) \to (a = b)\ )$
Transitivity	$\forall a \in \mathbb{R}\ \forall b \in \mathbb{R}\ \forall c \in \mathbb{R}\ (\ (a \leq b \wedge b \leq c)\ \to\ (a \leq c)\ )$
Trichotomy	$\forall a \in \mathbb{R}\ \forall b \in \mathbb{R}\ (\ (a = b\ \vee\ b > a\ \vee\ a < b)$

Completeness axioms (Rosen Appendix 1):

Least upper bound	Every nonempty set of real numbers that is bounded above has a least upper bound
Nested intervals	For each sequence of intervals $[a_n, b_n]$ where, for each n, $a_n < a_{n+1} < b_{n+1} < b_n$, there is at least one real number x such that, for all n, $a_n \leq x \leq b_n$.

Each real number $r \in \mathbb{R}$ is described by a function to give better and better approximations

$$x_r : \mathbb{Z}^+ \to \{0, 1\} \qquad \text{where } x_r(n) = n^{th} \text{ bit in binary expansion of } r$$

r	Binary expansion	x_r
0.1	$0.00011001\ldots$	$x_{0.1}(n) = \begin{cases} 0 & \text{if } n > 1 \text{ and } (n \textbf{ mod } 4) = 2 \\ 0 & \text{if } n = 1 \text{ or if } n > 1 \text{ and } (n \textbf{ mod } 4) = 3 \\ 1 & \text{if } n > 1 \text{ and } (n \textbf{ mod } 4) = 0 \\ 1 & \text{if } n > 1 \text{ and } (n \textbf{ mod } 4) = 1 \end{cases}$
$\sqrt{2} - 1 = 0.4142135\ldots$	$0.01101010\ldots$	Use linear approximations (tangent lines from calculus) to get algorithm for bounding error of successive operations. Define $x_{\sqrt{2}-1}(n)$ to be n^{th} bit in approximation that has error less than $2^{-(n+1)}$.

Claim: $\{r \in \mathbb{R} \mid 0 \leq r \land r \leq 1\}$ is uncountable.

Approach 1: Mimic proof that $\mathcal{P}(\mathbb{Z}^+)$ is uncountable.

Proof: By definition of countable, since $\{r \in \mathbb{R} \mid 0 \leq r \land r \leq 1\}$ is not finite, **to show** is $|\mathbb{N}| \neq |\{r \in \mathbb{R} \mid 0 \leq r \land r \leq 1\}|$.

To show is $\forall f : \mathbb{Z}^+ \to \{r \in \mathbb{R} \mid 0 \leq r \land r \leq 1\}$ (f is not a bijection) . Towards a proof by universal generalization, consider an arbitrary function $f : \mathbb{Z}^+ \to \{r \in \mathbb{R} \mid 0 \leq r \land r \leq 1\}$. **To show**: f is not a bijection. It's enough to show that f is not onto. Rewriting using the definition of onto, **to show**:

$$\exists x \in \{r \in \mathbb{R} \mid 0 \leq r \land r \leq 1\} \, \forall a \in \mathbb{N} \; (\; f(a) \neq x \;)$$

In search of a witness, define the following real number by defining its binary expansion

$$d_f = 0.b_1 b_2 b_3 \cdots$$

where $b_i = 1 - b_{ii}$ where b_{jk} is the coefficient of 2^{-k} in the binary expansion of $f(j)$. Since[1] $d_f \neq f(a)$ for any positive integer a, f is not onto.

Approach 2: Nested closed interval property

To show $f : \mathbb{N} \to \{r \in \mathbb{R} \mid 0 \leq r \land r \leq 1\}$ is not onto. **Strategy**: Build a sequence of nested closed intervals that each avoid some $f(n)$. Then the real number that is in all of the intervals can't be $f(n)$ for any n. Hence, f is not onto.

Consider the function $f : \mathbb{N} \to \{r \in \mathbb{R} \mid 0 \leq r \land r \leq 1\}$ with $f(n) = \frac{1+\sin(n)}{2}$

n	$f(n)$	Interval that avoids $f(n)$
0	0.5	
1	$0.920735\ldots$	
2	$0.954649\ldots$	
3	$0.570560\ldots$	
4	$0.121599\ldots$	
$\vdots$		

[1] There's a subtle imprecision in this part of the proof as presented, but it can be fixed.

Least greatest proofs

For a set of numbers X, how do you formalize "there is a greatest X" or "there is a least X"?

Prove or **disprove**: There is a least prime number.

Prove or **disprove**: There is a greatest integer.

Approach 1, De Morgan's and universal generalization:

Approach 2, proof by contradiction:

Extra examples: Prove or disprove that $\mathbb{N}$, $\mathbb{Q}$ each have a least and a greatest element.

Gcd definition

Definition: **Greatest common divisor** Let a and b be integers, not both zero. The largest integer d such that d is a factor of a and d is a factor of b is called the greatest common divisor of a and b and is denoted by $gcd(\ (a,b)\ )$.

Gcd examples

Why do we restrict to the situation where a and b are not both zero?

Calculate $gcd(\ (10,15)\ )$

Calculate $gcd(\ (10,20)\ )$

Gcd basic claims

Claim: For any integers a, b (not both zero), $gcd(\ (a, b)\ ) \geq 1$.

Proof: *Show that 1 is a common factor of any two integers, so since the gcd is the greatest common factor it is greater than or equal to any common factor.*

Claim: For any positive integers a, b, $gcd(\ (a, b)\ ) \leq a$ and $gcd(\ (a, b)\ ) \leq b$.

Proof *Using the definition of gcd and the fact that factors of a positive integer are less than or equal to that integer.*

Claim: For any positive integers a, b, if a divides b then $gcd(\ (a, b)\ ) = a$.

Proof *Using previous claim and definition of gcd.*

Claim: For any positive integers a, b, c, if there is some integer q such that $a = bq + c$,

$$gcd(\ (a, b)\ ) = gcd(\ (b, c)\ )$$

Proof *Prove that any common divisor of* a, b *divides* c *and that any common divisor of* b, c *divides* a.

Gcd lemma relatively prime

Lemma: For any integers p, q (not both zero), $gcd\left(\left(\frac{p}{gcd(\ (p,q)\ )}, \frac{q}{gcd(\ (p,q)\ )}\right)\right) = 1$. In other words, can reduce to relatively prime integers by dividing by gcd.

Proof:

Let x be arbitrary positive integer and assume that x is a factor of each of $\frac{p}{gcd(\ (p,q)\ )}$ and $\frac{q}{gcd(\ (p,q)\ )}$. This gives integers α, β such that

$$\alpha x = \frac{p}{gcd(\ (p,q)\ )} \qquad \beta x = \frac{q}{gcd(\ (p,q)\ )}$$

Multiplying both sides by the denominator in the RHS:

$$\alpha x \cdot gcd(\ (p,q)\ ) = p \qquad \beta x \cdot gcd(\ (p,q)\ ) = q$$

In other words, $x \cdot gcd(\ (p,q)\ )$ is a common divisor of p, q. By definition of gcd, this means

$$x \cdot gcd(\ (p,q)\ ) \leq gcd(\ (p,q)\ )$$

and since $gcd(\ (p,q)\ )$ is positive, this means, $x \leq 1$.

Sets numbers subsets

We have the following subset relationships between sets of numbers:

$$\mathbb{Z}^+ \subsetneq \mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$$

Which of the proper subset inclusions above can you prove?

Definitions set prereqs

Term	**Notation Example(s)**	**We say in English ...**
all reals	$\mathbb{R}$	The (set of all) real numbers (numbers on the number line)
all integers	$\mathbb{Z}$	The (set of all) integers (whole numbers including negatives, zero, and positives)
all positive integers	$\mathbb{Z}^+$	The (set of all) strictly positive integers
all natural numbers	$\mathbb{N}$	The (set of all) natural numbers. **Note**: we use the convention that 0 is a natural number.

Defining sets

To define sets:

To define a set using **roster method**, explicitly list its elements. That is, start with { then list elements of the set separated by commas and close with }.

To define a set using **set builder definition**, either form "The set of all x from the universe U such that x is ..." by writing

$$\{x \in U \mid ...x...\}$$

or form "the collection of all outputs of some operation when the input ranges over the universe U" by writing

$$\{...x... \mid x \in U\}$$

We use the symbol $\in$ as "is an element of" to indicate membership in a set.

Example sets: For each of the following, identify whether it's defined using the roster method or set builder notation and give an example element.

Can we infer the data type of the example element from the notation?

$\{-1, 1\}$

$\{0, 0\}$

$\{-1, 0, 1\}$

$\{(x, x, x) \mid x \in \{-1, 0, 1\}\}$

$\{\}$

$\{x \in \mathbb{Z} \mid x \geq 0\}$

$\{x \in \mathbb{Z} \mid x > 0\}$

$\{\smile, \sun\}$

$\{\mathtt{A}, \mathtt{C}, \mathtt{U}, \mathtt{G}\}$

$\{\mathtt{AUG}, \mathtt{UAG}, \mathtt{UGA}, \mathtt{UAA}\}$

Set operations

To define a set we can use the roster method, set builder notation, a recursive definition, and also we can apply a set operation to other sets.

New! Cartesian product of sets and **set-wise concatenation of sets of strings**

Definition: Let X and Y be sets. The **Cartesian product** of X and Y, denoted $X \times Y$, is the set of all ordered pairs (x, y) where $x \in X$ and $y \in Y$

$$X \times Y = \{(x, y) \mid x \in X \text{ and } y \in Y\}$$

Conventions: (1) Cartesian products can be chained together to result in sets of n-tuples and (2) When we form the Cartesian product of a set with itself $X \times X$ we can denote that set as X^2, or X^n for the Cartesian product of a set with itself n times for a positive integer n.

Definition: Let X and Y be sets of strings over the same alphabet. The **set-wise concatenation** of X and Y, denoted $X \circ Y$, is the set of all results of string concatenation xy where $x \in X$ and $y \in Y$

$$X \circ Y = \{xy \mid x \in X \text{ and } y \in Y\}$$

Pro-tip: the meaning of writing one element next to another like xy depends on the data-types of x and y. When x and y are strings, the convention is that xy is the result of string concatenation. When x and y are numbers, the convention is that xy is the result of multiplication. This is (one of the many reasons) why is it very important to declare the data-type of variables before we use them.

Fill in the missing entries in the table:

Set	**Example elements in this set and their data type**:
B	$\texttt{A} \quad \texttt{C} \quad \texttt{G} \quad \texttt{U}$
	$(\texttt{A}, \texttt{C}) \qquad (\texttt{U}, \texttt{U})$
$B \times \{-1, 0, 1\}$	
$\{-1, 0, 1\} \times B$	
	$(0, 0, 0)$
$\{\texttt{A}, \texttt{C}, \texttt{G}, \texttt{U}\} \circ \{\texttt{A}, \texttt{C}, \texttt{G}, \texttt{U}\}$	
	$\texttt{GGGG}$

Definitions functions prereqs

Term	Notation Example(s)	We say in English ...
sequence	$x_1, \ldots, x_n$	A sequence x_1 to x_n
summation	$\sum_{i=1}^{n} x_i$ or $\displaystyle\sum_{i=1}^{n} x_i$	The sum of the terms of the sequence x_1 to x_n
piecewise rule definition	$f(x) = \begin{cases} \text{rule 1 for } x & \text{when COND 1} \\ \text{rule 2 for } x & \text{when COND 2} \end{cases}$	Define f of x to be the result of applying rule 1 to x when condition COND 1 is true and the result of applying rule 2 to x when condition COND 2 is true. This can be generalized to having more than two conditions (or cases).
function application	$f(7)$	f of 7 **or** f applied to 7 **or** the image of 7 under f
	$f(z)$	f of z **or** f applied to z **or** the image of z under f
	$f(g(z))$	f of g of z **or** f applied to the result of g applied to z
absolute value	$\lvert -3 \rvert$	The absolute value of -3
square root	$\sqrt{9}$	The non-negative square root of 9

Pro-tip: the meaning of two vertical lines $\lvert \quad \rvert$ depends on the data-types of what's between the lines. For example, when placed around a number, the two vertical lines represent absolute value. We've seen a single vertial line $\mid$ used as part of set builder definitions to represent "such that". Again, this is (one of the many reasons) why is it very important to declare the data-type of variables before we use them.