Maths Exercise Sheet 5 Solutions
Sets and Cardinalities (and revision)

You do not have to answer all questions, but try to answer as many as you can.
Questions marked with one or more asterisks go beyond the scope of the course in difficulty or topic.

Note that answers to Question 3 may be submitted for feedback.

1. How many surjections are there from $\{0,1,2\}$ to $\{0,1\}$?

   A function $f : \{0,1,2\} \to \{0,1\}$ is completely determined by

   $$f^{-1}(\{0\}) = \{x \in \{0,1,2\} \mid f(x) = 0\},$$

   the set of elements that map to 0. This is because everything is sent to either 0 or 1.

   When f is a surjection, $f^{-1}(\{0\})$ contains at least one element because 0 is in the image of f, but it also contains at most two elements because 1 needs to be in the image of f.

   We can also go backwards. If $A \subseteq \{0,1,2\}$ and $1 \leq |A| \leq 2$, then we can find a surjection $f : \{0,1,2\} \to \{0,1\}$ with $f^{-1}(\{0\})) = A$, by mapping everything in A to 0 and everything in $\{0,1,2\} \backslash A$ to 1.

   So the problem is equivalent to counting the subsets of $\{0,1,2\}$ which have either 1 or 2 elements. This is

   $$\binom{3}{1} + \binom{3}{2} = 3 + 3 = \underline{6}.$$

   [What we did here was to construct a bijection

   $$\{\text{surjections } \{0,1,2\} \to \{0,1\}\} \to \{A \in P(\{0,1,2\}) \mid 1 \leq |A| \leq 2\}$$

   where the RHS is an easier set to count.]

2. Which of the following sets are countable and which are uncountable?

   (a) $\{2^n \mid n \in \mathbb{N}\}$
   Countable, because it's a subset of $\mathbb{N}$.

   (b) $\{n \in \mathbb{Z} \mid n \equiv 3 \pmod 7\}$
   Countable, because it's a subset of $\mathbb{Z}$, and we know that $\mathbb{Z}$ is countable.

   (c) $\mathbb{N} \times \mathbb{R}$
   Uncountable. To see this, consider

   $$\begin{aligned} \mathbb{R} &\to \mathbb{N} \times \mathbb{R} \\ x &\mapsto (0, x) \end{aligned}$$

   which is an injection from an uncountable set ($\mathbb{R}$) into our set.

(d) $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$
Countable (despite being a subset of $\mathbb{R}$).
Method 1: as a countable union of countable sets:

$$\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} = \bigcup_{a \in \mathbb{Q}} \{a + b\sqrt{2} \mid b \in \mathbb{Q}\}.$$

For fixed $a \in \mathbb{Q}$, we have a bijection

$$\begin{aligned} \mathbb{Q} &\to \{a + b\sqrt{2} \mid b \in \mathbb{Q}\} \\ b &\mapsto a + b\sqrt{2} \end{aligned}$$

so we are dealing with a union of countable sets. But the indexing set is $\mathbb{Q}$, which is countable, so the whole thing is rational.
Method 2: Product of countable sets: The function

$$\begin{aligned} \mathbb{Q} \times \mathbb{Q} &\to \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \\ (a, b) &\mapsto a + b\sqrt{2} \end{aligned}$$

is a surjection, so there is a subset of $\mathbb{Q} \times \mathbb{Q}$ which bijects with the other set. But $\mathbb{Q} \times \mathbb{Q}$ is countable. [In fact, a short extra argument using the irrationality of $\sqrt{2}$ shows that this map is a bijection.]

(e) $\mathbb{R}^{\mathbb{R}}$
Uncountable. There is an injection $\mathbb{R} \to \mathbb{R}^{\mathbb{R}}$ which sends a real number α to the function $f_\alpha : \mathbb{R} \to \mathbb{R}$ defined by $f_\alpha(x) = \alpha$ for all $x \in \mathbb{R}$. Using lambda-notation:

$$\begin{aligned} \mathbb{R} &\to \mathbb{R}^{\mathbb{R}} \\ \alpha &\mapsto \lambda x.\alpha \end{aligned}$$

(f) $\{A \in P(\mathbb{N}) \mid A \text{ is finite}\}$
Countable. If $A \subseteq \mathbb{N}$ is finite, then $A \subseteq \{x \in \mathbb{N} \mid x < n\}$ for some natural number $n \in \mathbb{N}$. For each such n there are only finitely many subsets. So

$$\{A \in P(\mathbb{N}) \mid A \text{ is finite}\} = \bigcup_{n \in \mathbb{N}} P(\{x \in \mathbb{N} \mid x < n\})$$

is a countable union of finite sets.

** (g) $\{A \in P(\mathbb{Z}) \mid \forall x, y \in A.\, x - y \in A\}$.
Countable (despite being a subset of $P(\mathbb{Z})$). The idea is to recognize that the condition on A is quite strong.

- A could be empty.
- If A is non-empty, then $0 \in A$ (because if any $x \in A$ then $0 = x - x \in A$).
- If $x \in A$, then $-x \in A$ (because $-x = 0 - x$).
- If $x, y \in A$, then $x + y \in A$ (because $x + y = x - (-y)$).
- If $x, y \in A$, then $ax + by \in$ for all $a, b \in \mathbb{Z}$ (iterating the ideas above).
- Hence, if $x, y \in A$, then $\gcd(x, y) \in A$.

Lemma: Either A is empty or $A = \{kn \mid k \in \mathbb{Z}\}$ for some $n \in \mathbb{N}$.
Proof: Suppose $A \neq \emptyset$ or $\{0\}$. Then A contains at least one positive integer. Let n be the least positive integer in A. Then certainly $\{kn \mid k \in \mathbb{Z}\} \subseteq A$. Moreover, if $y \in A$, then $\gcd(n, y) \in A$, where $1 \leq \gcd(n, y) \leq n$. But since n was the least positive integer in A, we must have $\gcd(n, y) = n$. In other words, y is a multiple of n, so $A \subseteq \{kn \mid k \in \mathbb{Z}\}$. □
Now there are clearly only countably many possibilities for sets A of this form.

3. **(Feedback)** For both of the following sets, find whether they are countable or uncountable. [You may quote results from lectures without proof. As always, explain your reasoning carefully.]
   (a) $\{A \subseteq \mathbb{N} \mid 0 \notin A\}$ (b) $\{f : \mathbb{N} \to \mathbb{N} \mid \forall n \in \mathbb{N}. f(n+1) = f(n) + 1\}$

4. (a) Let X be any set. Show that $A \mapsto X \backslash A$ is a bijection $P(X) \to P(X)$.
   Method 1: A function is bijection iff it is has an inverse function. We can show that $A \mapsto X \backslash A$ is its own inverse function. For $x \in X$,

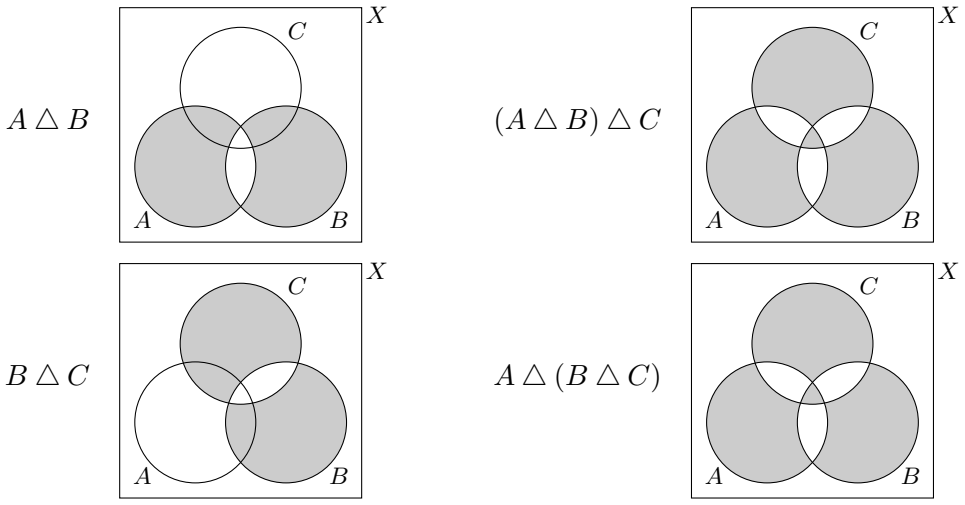
$$\begin{aligned} x \in X\backslash(X\backslash A) &\iff x \notin X\backslash A \\ &\iff x \in A, \end{aligned}$$

   so $X\backslash(X\backslash A) = A$ because they have the same elements.
   Method 2: We just have to check that it is both injective and surjective.
   Injective: Let $A, B \subseteq X$, and suppose $X\backslash A = X\backslash B$. Then

$$x \in A \iff x \in X \wedge x \notin X\backslash A \iff x \in X \wedge x \notin X\backslash B \iff x \in B.$$

   So A and B have the same elements, so they are equal.
   Surjective: Let $C \subseteq X$. We want to show there exists $A \subseteq X$ such that $X\backslash A = C$. Let's try $A = X\backslash C$. What we need to check that $X\backslash(X\backslash C) = C$, see the calculation from Method 1.

   (b) Prove that the symmetric difference $\triangle$ is an associative operation $P(X)^2 \to P(X)$. Is it commutative? Does it have a neutral element? If $\triangle$ were 'addition', would it have negatives?
   This is quite an involved calculation if you try to do it symbolically, so don't worry if you got lost. You will not have any exam questions that require this much work. The most reliable approach to convincing yourself of the associativity is probably by drawing Venn diagrams, but it is hard to communicate this as a written proof. There is a difficult calculation in terms of logic/Boolean algebra, but there is also an elegant algebraic way to solve the problem using arithmetic modulo 2. Following any approach, you might notice that $(A \triangle B) \triangle C$ and $A \triangle (B \triangle C)$ both represent the set of elements of X that are present in an *odd* number of A, B, C.
   Method 1: Check associativity by drawing Venn diagrams.
   To compute the Venn diagram of $(A \triangle B) \triangle C$), first look at the Venn diagram for $A \triangle B$, and then flip the colour of each region contained in C. Do similarly for $A \triangle (B \triangle C)$.



Now it's clear that $(A \triangle B) \triangle C = A \triangle (B \triangle C)$. For commutativity, note that if we drew a Venn diagram of $B \triangle A$, it would be exactly the same as the one for $A \triangle B$, so $\triangle$ is commutative.

The neutral element is the emptyset, since

$$\begin{aligned} x \in A \triangle \emptyset &\iff (x \in A \wedge x \notin \emptyset) \vee (x \notin A \wedge x \in \emptyset) \\ &\iff x \in A. \end{aligned}$$

For negatives, every element is its own negative:

$$\begin{aligned} x \in A \triangle A &\iff (x \in A \wedge x \notin A) \vee (x \notin A \wedge x \in A) \\ &\iff x \in A \wedge x \notin A \end{aligned}$$

but this is impossible, so $A \triangle A = \emptyset$.

Method 2: Check associativity using logic/Boolean algebra. We need to check $(A \triangle B) \triangle C = A \triangle (B \triangle C)$. For $x \in X$,

$$\begin{aligned} x \in (A \triangle B) \triangle C &\iff (x \in (A \triangle B) \wedge x \notin C) \vee (x \notin (A \triangle B) \wedge x \in C) \\ &\iff (((x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B)) \wedge x \notin C) \\ &\qquad \vee (((x \in A \wedge x \in B) \vee (x \notin A \wedge x \notin B)) \wedge x \in C) \\ &\iff (x \in A \wedge x \notin B \wedge x \notin C) \vee (x \notin A \wedge x \in B \wedge x \notin C) \\ &\qquad \vee (x \notin A \wedge x \notin B \wedge x \in C) \vee (x \in A \wedge x \in B \wedge x \in C) \end{aligned}$$

where we have put the logical condition into Disjunctive Normal Form. We can do the same with $x \in A \triangle (B \triangle C)$, and we will get the same condition. Note that this condition says that x is a member of precisely one of the sets A, B, C or else of all three of them.

The rest of the answer is as in Method 1.

Method 3: Reduce to arithmetic modulo 2.

Recall that for every subset $A \subseteq X$ we have a *characteristic function* $\chi_A : X \to \{0, 1\}$.

Lemma: $\chi_{A \triangle B}(x) \equiv \chi_A(x) + \chi_B(x) \pmod 2$.

Proof: This is just a way of saying that $x \in A \triangle B$ iff x is in precisely one of A or B. □

Associativity: We work modulo 2:

$$\begin{aligned} \chi_{(A \triangle B) \triangle C}(x) &\equiv \chi_{A \triangle B}(x) + \chi_C(x) \pmod 2 \\ &\equiv (\chi_A(x) + \chi_B(x)) + \chi_C(x) \pmod 2 \\ &\equiv \chi_A(x) + (\chi_B(x) + \chi_C(x)) \pmod 2 \\ &\equiv \chi_A(x) + \chi_{B \triangle C}(x) \pmod 2 \\ &\equiv \chi_{A \triangle (B \triangle C)}(x) \pmod 2 \end{aligned}$$

But the first and last expressions are in $\{0, 1\}$, so if the are congruent modulo 2 they are actually equal. This proves associativity.

Commutativity:

$$\begin{aligned} \chi_{A \triangle B}(x) &\equiv \chi_A(x) + \chi_B(x) \pmod 2 \\ &\equiv \chi_B(x) + \chi_A(x) \pmod 2 \\ &\equiv \chi_{B \triangle A}(x) \pmod 2 \end{aligned}$$

Neutral element: Note that $\chi_\emptyset(x) = 0$, so $\chi_{A \triangle \emptyset}(x) \equiv \chi_A(x) + \chi_\emptyset(x) \equiv \chi_A(x) \pmod 2$.

Negatives: For $A \subseteq X$, we want to find $B \subseteq X$ such that $\chi_A(x) + \chi_B(x) \equiv 0 \pmod 2$. So obviously $B = A$ works.

5. Show that $(m, n) \mapsto 2^m(2n+1) - 1$ gives a bijection $\mathbb{N}^2 \to \mathbb{N}$.

   Injectivity: Suppose $2^{m_1}(2n_1+1) - 1 = 2^{m_2}(2n_2+1) - 1$. Adding 1 to both sides, we just have

   $$2^{m_1}(2n_1+1) = 2^{m_2}(2n_2+1)$$

   Now $2n_1+1$ and $2n_2+1$ are both odd, so are coprime to any power of 2. Thus we must have $2^{m_1} = 2^{m_2}$ and $2n_1+1 = 2n_2+1$. These imply that $m_1 = m_2$ and $n_1 = n_2$.

   Surjectivity: We want to show that each $N \in \mathbb{N}$ is in the image. If $N \in \mathbb{N}$, then $N+1 \geq 1$, so $N+1$ has a prime factorization. The important point is that it is a product of a power of 2 and an odd number, say $N+1 = 2^m(2n+1)$. But that means that N is the image of (m, n) under the function.

6. Give an explicit injection $\{0,1\}^* \to \{0,1\}^{\mathbb{N}}$. Is there an injection the other way round?

   There are many possible answers. The important thing is not to fall into the trap of doing something like mapping each string $a_0 a_1 \ldots_{n-1}$ to the stream $(a_0, a_1, \ldots, a_{n-1}, 0, 0, \ldots)$, because this would not be an injection.

   A simple way to avoid the trap is to encode the length of the string first before listing the digits. Something like

   $$a_0 a_1, \ldots a_{n-1} \mapsto (\underbrace{1, 1, \ldots, 1}_{n}, 0, a_0, a_1, \ldots, a_{n-1}, 0, 0, \ldots).$$

   In words, a string s of length n is mapped to the stream which begins with n 1's, then a 0, then the next n digits are the string s, and from then on is just 0's.

   There is no injection the other way round, because we saw that $\{0,1\}^{\mathbb{N}}$ is uncountable whereas $\{0,1\}^*$ is countable.

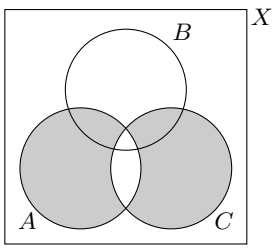
7. Consider the relation R on $P(\mathbb{N})$ given by $R = \{(A, B) \in P(\mathbb{N})^2 \mid A \triangle B \text{ is finite}\}$. Show that R is an equivalence relation. ** Is $P(\mathbb{N})/R$ countable or uncountable?

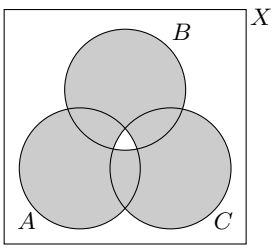
   - Reflexive: $A \triangle A = \emptyset$ which is finite, so $A \; R \; A$ for any $A \in P(\mathbb{N})$.
   - Symmetric: $B \triangle A = A \triangle B$, so the LHS is finite iff the RHS is finite.
   - Transitive: Suppose $A \triangle B$ and $B \triangle C$ are both finite. Then

     $$A \triangle C \subseteq (A \triangle B) \cup (B \triangle C)$$

     so $A \triangle C$ is a subset of a union of two finite sets, so is itself finite.

   The inclusion of sets $A \triangle C \subseteq (A \triangle B) \cup (B \triangle C)$ can be pictured with Venn diagrams:

   $A \triangle B =$ 

   $\subseteq$ 

   $= (A \triangle B) \cup (B \triangle C)$

   For the last part, the quotient will turn out to be uncountable.

   Lemma: Each equivalence class of R is countable.
   Proof: For $A \in P(\mathbb{N})$ there is a bijection between $[A]_R$ and the set of finite subsets of $\mathbb{N}$:

   $$[A]_R \to \{A \in P(\mathbb{N}) \mid A \text{ finite}\}$$
   $$B \mapsto A \triangle B$$

This is well-defined, since by definition if $A\ R\ B$ then their symmetric difference is finite. It is injective since, by Q4(b), $\triangle$ admits 'negatives', so given $A \triangle B_1 = A \triangle B_2$, we can take $A \triangle (-)$ of both sides to get $B_1 = B_2$. It is surjective since if $F \subseteq \mathbb{N}$ is a finite set, then

$$A \triangle (A \triangle F) = F$$

is finite so $A\ R\ (A \triangle F)$. Thus the element $A \triangle F \in [A]_R$ is mapped to F. This proves the lemma, since bt Q2(f), $\{A \in P(\mathbb{N}) \mid A \text{ finite}\}$ is countable. □

Now, the equivalence classes partition $P(\mathbb{N})$, so in particular we have

$$P(\mathbb{N}) = \bigcup_{C \in P(\mathbb{N})/R} C.$$

But each class C is *countable*, and $P(\mathbb{N})$ is *uncountable*, therefore the indexing set of the union must be *uncountable*, because a countable union of countable sets would again be countable. So $P(\mathbb{N})/R$ is uncountable.

8. (a) Construct an explicit bijection between $\{0,1\}^{\mathbb{N}}$ and $\{0,1,2,3\}^{\mathbb{N}}$.
Intuitively, the idea is that

$$\begin{aligned}\{0,1\}^{\mathbb{N}} &\approx \{0,1\} \times \{0,1\} \times \{0,1\} \times \{0,1\} \times \{0,1\} \times \{0,1\} \times \dots \\ &\approx (\{0,1\} \times \{0,1\}) \times (\{0,1\} \times \{0,1\}) \times (\{0,1\} \times \{0,1\}) \times \dots \\ &\approx (\{0,1\} \times \{0,1\})^{\mathbb{N}}.\end{aligned}$$

Let us define

$$\begin{aligned}\{0,1\}^{\mathbb{N}} &\to \{0,1,2,3\}^{\mathbb{N}} \\ f &\mapsto \lambda n.\, f(2n) + 2f(2n+1).\end{aligned}$$

(b) Deduce that there exists a bijection between $\{0,1\}^{\mathbb{N}}$ and $\{0,1,2\}^{\mathbb{N}}$.
There is obvious an injection (an inclusion even)

$$\{0,1\}^{\mathbb{N}} \to \{0,1,2\}^{\mathbb{N}}$$

and another

$$\{0,1,2\}^{\mathbb{N}} \to \{0,1,2,3\}^{\mathbb{N}}.$$

But, composing the latter with the bijection $\{0,1,2,3\}^{\mathbb{N}} \to \{0,1\}^{\mathbb{N}}$, we get an injection

$$\{0,1,2\}^{\mathbb{N}} \to \{0,1\}^{\mathbb{N}}.$$

Since we have injections both ways, the Cantor-Schröder-Bernstein Theorem tells us that there is a bijection.

9. Consider binary operations $\oplus, \otimes : (\mathbb{R}^2)^2 \to \mathbb{R}^2$ on $\mathbb{R}^2$ given by

$$(a,b) \oplus (c,d) = (a+c, b+d) \qquad (a,b) \otimes (c,d) = (ac - bd, ad + bc).$$

Show that these operations make $\mathbb{R}^2$ a field. [Optional hint: The neutral element for $\oplus$ will be $(0,0)$. The reciprocal of a non-zero (a,b) will be $(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2})$.]

This question is an introduction to complex numbers. If we think of pairs like $(a,0)$ as representing the real number a, then the point is that $(0,1)$ is now a square root of -1 (because $(0,1) \otimes (0,1) = (-1,0)$). So a pair (a,b) is what is usually written something like $a + ib$ when thought of as a complex number. The calculations are a little involved, but are good to try for yourself at least once.

- Associativity of $\oplus$: (this one is fairly obvious from the formula, but here it is written out anyway)

$$\begin{aligned}((a,b)\oplus(c,d))\oplus(e,f) &= (a+c,b+d)\oplus(e,f)\\ &= ((a+c)+e,(b+d)+f)\\ &= (a+(c+e),b+(d+f))\\ &= (a,b)\oplus(c+e,d+f)\\ &= (a,b)\oplus((c,d)\oplus(e,f))\end{aligned}$$

- Associativity of $\otimes$:

$$\begin{aligned}&((x_1,x_2)\otimes(y_1,y_2))\otimes(z_1,z_2)\\ &= (x_1y_1-x_2y_2,x_1y_2+x_2y_1)\otimes(z_1,z_2)\\ &= ((x_1y_1-x_2y_2)z_1-(x_1y_2+x_2y_1)z_2,(x_1y_1-x_2y_2)z_2+(x_1y_2+x_2y_1)z_1)\\ &= (x_1y_1z_1-(x_2y_2z_1+x_1y_2z_2+x_2y_1z_2),(x_1y_1z_2+x_1y_2z_1+x_2y_1z_1)-x_2y_2z_2)\end{aligned}$$

  and you get the same result if you start from $(x_1,x_2)\otimes((y_1,y_2)\otimes(z_1,z_2))$.
- Commutativity: for $\oplus$ this is obvious. For $\otimes$, just write out both formulas

$$\begin{aligned}(x_1,x_2)\otimes(y_1,y_2) &= (x_1y_1-x_2y_2,x_1y_2+x_2y_1)\\ (y_1,y_2)\otimes(x_1,x_2) &= (y_1x_1-y_2x_2,y_1x_2+y_2x_1)\end{aligned}$$

  and note that these are equal up to commuting the addition and multiplication of real numbers.
- Neutral elements: The 'zero' is $(0,0)$ and the 'one' is $(1,0)$:

$$\begin{aligned}(a,b)\oplus(0,0) &= (a+0,b+0)\\ &= (a,b)\\ (a,b)\otimes(1,0) &= (a\times1-b\times0,a\times0+b\times1)\\ &= (a-0,0+b)\\ &= (a,b)\end{aligned}$$

- Distributivity:

$$\begin{aligned}(x_1,x_2)\otimes((y_1,y_2)\oplus(z_1,z_2)) &= (x_1,x_2)\otimes(y_1+z_1,y_2+z_2)\\ &= (x_1(y_1+z_1)-x_2(y_2+z_2),x_1(y_2+z_2)+x_2(y_1+z_1))\\ &= (x_1y_1+x_1z_1-x_2y_2-z_2z_2,x_1y_2+x_1y_2+x_2y_1+x_2z_1)\\ &= (x_1y_1-x_2y_2+x_1z_1-z_2z_2,x_1y_2+x_2y_1+x_1y_2+x_2z_1)\\ &= (x_1y_1-x_2y_2,x_1y_2+x_2y_1)\oplus(x_1z_1-z_2z_2,x_1y_2+x_2z_1)\\ &= ((x_1,x_2)\otimes(y_1,y_2))\oplus((x_1,x_2)\otimes(z_1,z_2))\end{aligned}$$

  In practice, you would probably check something like this by working from both ends of the equation at once and trying to meet in the middle.
- Negatives: $-(a,b)$ is just $(-a,-b)$.

$$\begin{aligned}(a,b)\oplus(-a,-b) &= (a+(-a),b+(-b))\\ &= (0,0)\end{aligned}$$

- Reciprocals: if (a, b) is non-zero, then the expression

$$\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$$

makes sense because the denominators of the fractions are non-zero. We just have to calculate to check the desired property.

$$\begin{aligned}(a,b) \otimes (\tfrac{a}{a^2+b^2}, \tfrac{-b}{a^2+b^2}) &= (a\tfrac{a}{a^2+b^2} - b\tfrac{-b}{a^2+b^2}, a\tfrac{-b}{a^2+b^2} + b\tfrac{a}{a^2+b^2})n \\ &= (\tfrac{a^2-(-b)b}{a^2+b^2}, \tfrac{a(-b)+ba}{a^2+b^2}) \\ &= (1,0)\end{aligned}$$

10. (a) Explain how you know there exists a bijection $\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ for any $m, n \in \mathbb{N}$, $m, n > 0$.
The two sets are finite and have the same number of elements, so there must be a bijection between them. In more detail, each $\mathbb{Z}_k$ is a set of residue classes, which we know correspond to possible residue (mod k). The possibilities are $0, 1, \ldots, k-1$, so $|\mathbb{Z}_k| = k$. Using the fact the the size of a product of two finite sets is just the product of their sizes, we have

$$|\mathbb{Z}_m \times \mathbb{Z}_n| = |\mathbb{Z}_m| \times |\mathbb{Z}_n| = mn = |\mathbb{Z}_{mn}|$$

****(b) When m and n are coprime, show that $[N]_{mn} \mapsto ([N]_m, [N]_n)$ is such a bijection.
This abstracts the method of solving simultaneous congruences. This statement, or a strengthened form of it, is known as the 'Chinese Remainder Theorem'.
Because it is a function defined on a quotient set, we need to check that it is well-defined before getting to injectivity and surjectivity.
Well-defined: Suppose $N_1 \equiv N_2 \pmod{mn}$. Then $mn \mid N_1 - N_2$, so also $m \mid N_1 - N_2$ and $n \mid N_1 - N_2$. This means that $N_1 \equiv N_2 \pmod{m}$ and $N_1 \equiv N_2 \pmod{n}$. Thus the pair $([N]_m, [N]_n)$ does not depend on the representative N chosen for the equivalence class $[N]_{mn}$.
Injective: Suppose $N_1 \equiv N_2 \pmod{m}$ and $N_1 \equiv N_2 \pmod{n}$. We need to show that $N_1 \equiv N_2 \pmod{mn}$. We have $N_1 - N_2 = km$ for some $k \in \mathbb{Z}$, and $n \mid km$. But m and n are coprime, so $n \mid k$. So $k = k'n$ for some $k' \in \mathbb{Z}$, and $N_1 - N_2 = k'mn$, $N_1 \equiv N_2 \pmod{mn}$.
Surjective: Let $x, y \in \mathbb{Z}$. We want to show that $([x]_m, [y]_n)$ is in the image of the function. To do this, find Bézout coefficients for m and n:

$$am + bn = 1$$

which we can do since m and n are coprime. Now let

$$z = amy + bnx.$$

We'll show that $[z]_{mn}$ is mapped to $([x]_m, [y]_n)$, i.e. that $z \equiv x \pmod{m}$ and $z \equiv y \pmod{n}$. But

$$\begin{aligned}z &= amx + bny \\ &\equiv bny \pmod{m} \\ &\equiv (1 - am)y \pmod{m} \\ &\equiv y \pmod{m}\end{aligned}$$

and

$$\begin{aligned} z &= amx + bny \\ &\equiv amx \pmod{n} \\ &\equiv (1 - bn)x \pmod{n} \\ &\equiv x \pmod{n} \end{aligned}$$

as required.

**11. A function $f : \mathbb{N} \to \mathbb{N}$ is decreasing if $f(n+1) \leq f(n)$ for all n. Is the set of decreasing functions $\mathbb{N} \to \mathbb{N}$ countable or uncountable? What about increasing functions?

The set of decreasing functions $\mathbb{N} \to \mathbb{N}$ is *countable*. One approach is to use induction to show that the set of decreasing functions with $f(0) = k$ is countable for all k. For the base case, if $f(0) = 0$, then f is a constant function with $f(n) = 0$ for all n, For the inductive step, if $f(0) = k + 1$ then either f is constant with $f(n) = k + 1$ for all n, or else there is an $N \in \mathbb{N}$ such that $f(N) \leq k$. Then the function $i \mapsto f(N + i)$ is a decreasing function which sends 0 to something $\leq k$, so there are only countably many possibilities. Thus we are looking at a countable union of countable sets.

Another approach is inject the set of decreasing functions into the set of finite subsets of $\mathbb{N} \times \mathbb{N}$:

$$f \mapsto \{(m, n) \in \mathbb{N}^2 \mid f(m + 1) + n = f(m) \wedge n > 0\}.$$

Since each decreasing function can only 'step down' finitely many times before getting stuck at zero, this is always finite set.

The set of increasing functions in *uncountable*. One approach is to inject the set of binary sequences into it:

$$\begin{aligned} \{0, 1\}^{\mathbb{N}} &\to \{\text{increasing functions } \mathbb{N} \to \mathbb{N}\} \\ (a_n)_n &\mapsto \lambda n. \sum_{i=0}^{n} a_i. \end{aligned}$$

One could also use a diagonal argument directly. Let $F : \mathbb{N} \to \{\text{increasing functions } \mathbb{N} \to \mathbb{N}\}$ be a bijection. Define

$$g(n) = \max\{F(0)(n), \ldots, F(n)(n)\} + 1$$

Then $g(n)$ is increasing and $g(n) > F(n)(n)$ for all n, so $g \neq F(n)$ for any n.

*[10]12. Define a relation $\sim$ on $\mathbb{Q}^{\mathbb{N}}$ by $(a_n) \sim (b_n)$ iff

$$\forall C \in \mathbb{N}. \exists N \in \mathbb{N}. \forall m, n \in \mathbb{N}. m, n > N \implies |a_m - b_n| < \frac{1}{C + 1}.$$

Show that the situation of Sheet 4 Q5 applies. Do you recognize $\mathbb{Q}^{\mathbb{N}}/\!\sim$?

We are asked to show that $\sim$ is symmetric and transitive. For symmetry there is nothing to show, because the formula is obvious symmetric in (a_n) and (b_n). For transitivity, suppose $(a_n) \sim (b_n)$ and $(b_n) \sim (c_n)$. We need to show

$$\forall C \in \mathbb{N}. \exists N \in \mathbb{N}. \forall m, n \in \mathbb{N}. m, n > N \implies |a_m - c_n| < \frac{1}{C + 1}.$$

So suppose we are given $C \in \mathbb{N}$. We have to show

$$\exists N \in \mathbb{N}. \forall m, n \in \mathbb{N}. m, n > N \implies |a_m - c_n| < \frac{1}{C + 1}.$$

By hypothesis, if we let $C' = 2C + 1$, we can find N_1 and N_2 such that

$$\forall m, n \in \mathbb{N}.\, m, n > N_1 \implies |a_m - b_n| < \frac{1}{C' + 1}.$$

and

$$\forall n, p \in \mathbb{N}.\, n, p > N_2 \implies |b_n - c_p| < \frac{1}{C' + 1}.$$

Let $N' = \max(N_1, N_2)$. We'll use N' as the witness to what we want to prove and then show

$$\forall m, n \in \mathbb{N}.\, m, n > N' \implies |a_m - c_n| < \frac{1}{C + 1}.$$

But if $m, n \in \mathbb{N}$ and $m, n > N'$, then certainly $m, n > N_1$ and $m, n > N_2$, and

$$\begin{aligned} |a_m - c_n| &\leq |a_m - b_{N'+1}| + |b_{N'+1} - c_n| \\ &< \frac{1}{C' + 1} + \frac{1}{C' + 1} \\ &= \frac{1}{2(C + 1)} + \frac{1}{2(C + 1)} = \frac{1}{C + 1} \end{aligned}$$

as required.

The sequences (a_n) satisfying $(a_n) \sim (a_n)$ are called *Cauchy sequences*. Each such sequence is supposed to determine a real number by 'converging' to it, however, each real number has many Cauchy sequences that converge to it. By quotienting by this partial equivalence relation, we get a concrete construction of $\mathbb{R}$.

This construction is quite sophisticated, but one very nice feature is how easy it is how transparent the algebraic operations are. Sums and products are just given 'elementwise' in the sequence. The existence of $\sqrt{2}$ follows by consider the equivalence class of any rational approximation sequence, e.g. $[(\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots)]$ using the Pell fractions from Sheet 4.